PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Ryu INADA

New U.S. Patent Application

Filed: August 31, 1999 Docket No.: 104116

For: METHOD FOR GROUP UNIT ENCRYPTION/DECRYPTION, AND METHOD AND APPARATUS FOR WRITING SIGNATURE

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 10-291879, filed October 14, 1999

In support of this claim, a certified copy of said original foreign application:

_X_ is filed herewith.

_____ was filed on _____ in Parent Application No. _____ filed _____.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/epb

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１０月１４日

出 願 番 号
Application Number: 平成１０年特許願第２９１８７９号

出 願 人
Applicant (s): 富士ゼロックス株式会社

１９９９年 ７月１２日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０４９０１０

【書類名】　特許願

【整理番号】　FK98-00046

【提出日】　平成10年10月14日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/30

【発明の名称】　グループ単位の暗号化・復号方法および署名方法ならびに装置

【請求項の数】　19

【発明者】

【住所又は居所】　神奈川県川崎市高津区坂戸３丁目２番１号　ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル　富士ゼロックス株式会社内

【氏名】　稲田　龍

【特許出願人】

【識別番号】　000005496

【氏名又は名称】　富士ゼロックス株式会社

【電話番号】　0462-38-8516

【代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　038818

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　グループ単位の暗号化・復号方法および署名方法ならびに装置

【特許請求の範囲】

【請求項１】　公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶するステップと、

上記錠データの公開鍵を用いて暗号化対象データを暗号化するステップとを有することを特徴とする暗号化方法。

【請求項２】　上記暗号化対象データは、暗号化された情報を復号するのに用いる復号鍵とする請求項１記載の暗号化方法。

【請求項３】　公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶するステップと、

上記錠データに含まれる上記暗号化共通鍵の１つを上記グループ・メンバの対応する秘密鍵で復号して上記共通鍵を生成するステップと、

上記錠データに含まれる上記暗号化秘密鍵を、上記復号した共通鍵を用いて復号して上記秘密鍵を生成するステップと、

上記公開鍵で暗号化した暗号化対象データを取得するステップと、

上記復号した秘密鍵を用いて、上記暗号化された暗号化対象データの復号を行なうステップとを有することを特徴とする暗号復号方法。

【請求項４】　公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶するステップと、

上記錠データに含まれる上記暗号化共通鍵の１つを上記グループ・メンバの対応する秘密鍵で復号して上記共通鍵を生成するステップと、

上記錠データに含まれる上記暗号化秘密鍵を、上記復号した共通鍵を用いて復号して上記秘密鍵を生成するステップと、

上記公開鍵で検証できる署名を行なう署名対象データを記憶する取得するステップと、

上記復号した秘密鍵を用いて、上記署名対象データに署名を行なうステップとを有することを特徴とする署名方法。

【請求項５】　対をなす公開鍵および秘密鍵を取得するステップと、

共通鍵を取得するステップと、

上記秘密鍵を上記共通鍵で暗号化して暗号化秘密鍵を生成するステップと、

上記共通鍵をグループ・メンバの各々の公開鍵で暗号化して対応する暗号化共通鍵を生成するステップと、

上記公開鍵、上記暗号化秘密鍵および上記暗号化共通鍵を組み合わせて錠データを生成するステップとを有することを特徴とする錠データ生成方法。

【請求項６】　対をなす公開鍵および秘密鍵を取得するステップと、

共通鍵を取得するステップと、

逆関数が存在する所定の関数を用いて上記秘密鍵を変形して変形秘密鍵を生成するステップと、

上記変形秘密鍵を上記共通鍵で暗号化して暗号化変形秘密鍵を生成するステップと、

上記共通鍵をグループ・メンバの各々の公開鍵で暗号化して対応する暗号化共通鍵を生成するステップと、

上記公開鍵、上記暗号化変形秘密鍵および上記暗号化共通鍵を組み合わせて錠データを生成するステップとを有することを特徴とする錠データ生成方法。

【請求項７】　対をなす公開鍵および秘密鍵を取得するステップと、

共通鍵を取得するステップと、

上記秘密鍵を上記共通鍵で暗号化して暗号化秘密鍵を生成するステップと、

グループ・メンバの各々の公開鍵に対して冗長データ生成用の関数を実行して冗長データを生成するステップと、

上記共通鍵および上記冗長データの組を上記グループ・メンバの各々の公開鍵で暗号化して対応する暗号化共通鍵を生成するステップと、

上記公開鍵、上記暗号化秘密鍵および上記暗号化共通鍵を組み合わせて錠データを生成するステップとを有することを特徴とする錠データ生成方法。

【請求項８】　上記錠データは、署名を検証するための公開鍵と、上記署名

を行なうための署名用秘密鍵を変更権限所有者の公開鍵で暗号化した暗号化署名用秘密鍵と、上記錠データに含まれる所定のデータに対する上記署名用秘密鍵による署名とをさらに含む請求項５、６または７記載の錠データ生成方法。

【請求項９】　第１の公開鍵と、上記第１の公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵と、署名を検証するための第２の公開鍵と、上記署名を行なうための署名用秘密鍵を変更権限所有者の公開鍵で暗号化した暗号化署名用秘密鍵と、上記第１の公開鍵、上記暗号化秘密鍵、上記暗号化共通鍵、上記第２の公開鍵および上記暗号化署名用秘密鍵に対して上記署名用秘密鍵を用いた行なった署名とを含んでなる錠データを記憶するステップと、

上記錠データに含まれる上記暗号化署名用秘密鍵を上記変更権限所有者の秘密鍵で復号して署名用秘密鍵を生成するステップと、

上記錠データを変更するステップと、

変更した錠データに対して上記署名用秘密鍵で署名を行なうステップとを有することを特徴とする錠データ変更方法。

【請求項１０】　上記錠データを変更するステップは、

上記第２の公開鍵を更新するステップと、

上記署名用秘密鍵を更新するステップと、

更新した署名用秘密鍵を上記変更権限所有者の公開鍵で暗号化して新たに生成した新たな暗号化署名用秘密鍵で、変更前の上記暗号化署名用秘密鍵を更新するステップと、

上記更新後の署名用秘密鍵で署名を行なうステップとを含む請求項９記載の錠データ変更方法。

【請求項１１】　上記錠データは上記錠データのバージョンを示すバージョン識別子を有する請求項９または１０記載の錠データ変更方法。

【請求項１２】　上記錠データは、前バージョン扱い識別子を有し、この識別子に基づいて前のバージョンの錠データの取り扱いを制御する請求項９、１０または１１記載の錠データ変更方法。

【請求項１３】　上記前バージョン扱い識別子は、上記錠データの変更の遡

及的適用の有無を識別する情報を含む請求項１２記載の錠データ変更方法。

【請求項１４】　公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなるグループ錠。

【請求項１５】　公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶する手段と、

上記錠データの公開鍵を用いて暗号化対象データを暗号化する手段とを有することを特徴とする暗号化装置。

【請求項１６】　公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶する手段と、

上記錠データに含まれる上記暗号化共通鍵の１つを上記グループ・メンバの対応する秘密鍵で復号して上記共通鍵を生成する手段と、

上記錠データに含まれる上記暗号化秘密鍵を、上記復号した共通鍵を用いて復号して上記秘密鍵を生成する手段と、

上記公開鍵で暗号化した暗号化対象データを取得する手段と、

上記復号した秘密鍵を用いて、上記暗号化された暗号化対象データの復号を行なう手段とを有することを特徴とする暗号復号装置。

【請求項１７】　公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶する手段と、

上記錠データに含まれる上記暗号化共通鍵の１つを上記グループ・メンバの対応する秘密鍵で復号して上記共通鍵を生成する手段と、

上記錠データに含まれる上記暗号化秘密鍵を、上記復号した共通鍵を用いて復号して上記秘密鍵を生成する手段と、

上記公開鍵で検証できる署名を行なう署名対象データを記憶する取得する手段と、

上記復号した秘密鍵を用いて、上記署名対象データに署名を行なう手段とを有

することを特徴とする署名装置。

【請求項１８】　対をなす公開鍵および秘密鍵を取得する手段と、

共通鍵を取得する手段と、

上記秘密鍵を上記共通鍵で暗号化して暗号化秘密鍵を生成する手段と、

上記共通鍵をグループ・メンバの各々の公開鍵で暗号化して対応する暗号化共通鍵を生成する手段と、

上記公開鍵、上記暗号化秘密鍵および上記暗号化共通鍵を組み合わせて錠データを生成する手段とを有することを特徴とする錠データ生成装置。

【請求項１９】　第１の公開鍵と、上記第１の公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵と、署名を検証するための第２の公開鍵と、上記署名を行なうための署名用秘密鍵を変更権限所有者の公開鍵で暗号化した暗号化署名用秘密鍵と、上記第１の公開鍵、上記暗号化秘密鍵、上記暗号化共通鍵、上記第２の公開鍵および上記暗号化署名用秘密鍵に対して上記署名用秘密鍵を用いた行なった署名とを含んでなる錠データを記憶する手段と、

上記錠データに含まれる上記暗号化署名用秘密鍵を上記変更権限所有者の秘密鍵で復号して署名用秘密鍵を生成する手段と、

上記錠データを変更する手段と、

変更した錠データに対して上記署名用秘密鍵で署名を行なう手段とを有することを特徴とする錠データ変更装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵暗号技術に関し、とくに、グループ・メンバのみ利用可能なグループ鍵を用いて復号や署名をグループの任意のメンバが行なえるようにしたものである。

【０００２】

【従来の技術】

公開鍵暗号と呼ばれる暗号方式が米国特許４，２００，７００号に記載されて

いる。公開鍵暗号は、平文を暗号化する際に用いる公開鍵と、暗号を平文に復号する際に用いる秘密鍵とを有する。公開鍵と秘密鍵とは異なる鍵であり、公開鍵は、文字通り公開され、公知の状態においておくことが可能である。従来の暗号方式（秘密鍵暗号、共通鍵暗号、慣用暗号ともいう）は、暗号化および復号に同一の鍵が使用されており、鍵の機密性を保つことが重要な課題であったが、この公開鍵暗号方式では、暗号化の鍵の機密性は不要となる。また、暗号文書を通信する人数がｎ人であった場合、従来の暗号化－復号共通鍵方式であるとｎ×（ｎ－１）÷２個の鍵が必要となるが、公開鍵暗号方式ではｎ個の鍵で済むといった利点がある。また、各人の署名、すなわち各人による秘密鍵による暗号化処理においても同じ枠組みを用いることができるといった特徴がある。例えば秘密鍵Ａを有する暗号通信メンバＰが、通信文Ｘを秘密鍵Ａで変換し、変換した文書Ｙと通信文Ｘを他のメンバＱに送付し、メンバＱは、メンバＰの公開鍵Ｂで変換文書Ｙを変換し、Ｙの変換結果がＸと一致すれば、その文書は、確かにメンバＰによって送付されたものであることが確認できる。このように公開鍵暗号方式には、従来の暗号方式には無いいくつかの優れた点を有する。

【０００３】

また、特開平７－２９７８１８号公報に、グループに対する公開鍵と秘密鍵の割り当てについての構成が記載されている。これは、カードのような物理的実態にグループ秘密鍵を埋め込み、カードをグループのメンバが確実に所持することを前提としたシステムである。すなわち、上述の秘密鍵と公開鍵の暗号システムをカードという実態を利用した構成とすることによって、個人という恒久的な存在から分離したカードという物理的実態を利用して鍵の管理を実現している。

【０００４】

【発明が解決しようとする課題】

公開鍵暗号方式では、個人のような恒久的な存在を独立した単位として設定している。従って、個人以外の例えば複数のメンバを一つの単位として設定する必要がある場合等には十分な機能を果たし得ない。また、上述のようなカードを使用したシステムにおいては、カードというハードウェアを用いなければならないこと、カード自体の管理の問題、カードの紛失、盗難等に起因するカード所有者

の正当性の問題、すなわちカード保有者がカードの正当な所有者であるかどうかの判断が困難であるという問題が発生する。

【０００５】

例えば、企業のように、部、課、あるいは係といった組織は協同作業単位であり、またそのような組織とは独立に成り立つタスクフォースといった複数の個人から構成される協同作業単位である。これら協同作業単位では、情報も共有される必要がある。すなわち、協同作業単位の内部と外部との関係では、情報の機密性を維持する必要があるが、内部の各メンバ間での情報の流通は必要となる。従って、その協同作業単位の任意の構成員が共有情報に対する復号処理、あるいは署名処理を行えるような暗号方式が必要となる。

【０００６】

さらに、協同作業単位の構成員は追加や削除といった変更が発生することがあるため、暗号方式は、これら構成員の変更にも対応可能な方式であることが必要である。また、協同作業単位と同様に、企業内における人事部長のような役割を果たすために、ある時点においてその役割を果たしている特定の個人とは独立な、すなわちその役割を果たしている個人の変更に対応可能な形で、その役割に応じた特定かつ継続的な機密状態を保持する必要がある。

【０００７】

本発明は上記の問題を解決する暗号方式を提供する。本発明は、公開鍵暗号方式を個人を単位とするのではなく、個人およびグループを要素とする集合であるグループにおいて使用可能とし、特定のグループに属する構成員（メンバ）が復号可能な暗号化方式を提供することを目的とする。

【０００８】

さらに本発明は、特定のグループに属する任意のメンバによる署名を可能とし、署名された文書がその特定グループに属するメンバによる署名であることを確認することが可能な署名方式を提供することを目的とする。

【０００９】

【課題を解決するための手段】

この発明によれば、以上の目的を達成するために、暗号化方法において、公開

鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶するステップと、上記錠データの公開鍵を用いて暗号化対象データを暗号化するステップとを実行するようにしている。

【００１０】

この構成においては、錠データに、暗号化用の公開鍵と、これに対応する秘密鍵を共通鍵で暗号化した暗号文と、上記共通鍵をグループ・メンバの公開鍵で暗号化した暗号文とを含ませているので、グループ・メンバは自分の秘密鍵を用いて共通鍵を取得し、さらにこの共通鍵で復号し暗号文を復号する秘密鍵を取得することができる。このような錠データの公開鍵で情報を暗号化することにより、グループ・メンバ以外に情報が漏れない態様で情報を送ることが可能になる。

【００１１】

また、この構成において、上記暗号化対象データを、暗号化された情報を復号するのに用いる復号鍵とすることができる。例えば、この復号鍵を共通鍵とし、いわゆる復号暗号スキームを実現できる。すなわち、錠データを用いて公開鍵暗合方式で共通鍵を暗号化してグループ・メンバに送付し、グループ・メンバは錠データでこれを復号する。そして共通鍵で暗号化された暗号文を、復号した共通鍵で復号する。

【００１２】

また、この発明によれば、上述の目的を達成するために、暗号復号方法において、公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶するステップと、上記錠データに含まれる上記暗号化共通鍵の１つを上記グループ・メンバの対応する秘密鍵で復号して上記共通鍵を生成するステップと、上記錠データに含まれる上記暗号化秘密鍵を、上記復号した共通鍵を用いて復号して上記秘密鍵を生成するステップと、上記公開鍵で暗号化した暗号化対象データを取得するステップと、上記復号した秘密鍵を用いて、上記暗号化された暗号化対象データの復号を行なうステップとを実行するようにしている。

【００１３】

この構成において、上述と同様に、グループ・メンバは錠データの秘密鍵を取得することができる。グループ・メンバであれば誰でも簡単に錠データの公開鍵で暗号化された暗号文を復号できる。しかも、グループ・メンバ以外は復号することができない。

また、この発明によれば、上述の目的を達成するために、署名方法において、公開鍵と、上記公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵とを含んでなる錠データを記憶するステップと、上記錠データに含まれる上記暗号化共通鍵の１つを上記グループ・メンバの対応する秘密鍵で復号して上記共通鍵を生成するステップと、上記錠データに含まれる上記暗号化秘密鍵を、上記復号した共通鍵を用いて復号して上記秘密鍵を生成するステップと、上記公開鍵で検証できる署名を行なう署名対象データを記憶する取得するステップと、上記復号した秘密鍵を用いて、上記署名対象データに署名を行なうステップとを実行するようにしている。

【００１４】

この構成においても、上述と同様に、錠データの公開鍵に対応する秘密鍵を取得できるのはグループ・メンバのみであるから、この秘密鍵を用いてデータに証明を行なうことにより、グループ・メンバの署名を行なうことができる。署名付きデータを取得した者は、錠データの公開鍵を用いて署名を検証できる。

【００１５】

また、この発明によれば、上述の目的を達成するために、錠データを生成する方法において、対をなす公開鍵および秘密鍵を取得するステップと、共通鍵を取得するステップと、上記秘密鍵を上記共通鍵で暗号化して暗号化秘密鍵を生成するステップと、上記共通鍵をグループ・メンバの各々の公開鍵で暗号化して対応する暗号化共通鍵を生成するステップと、上記公開鍵、上記暗号化秘密鍵および上記暗号化共通鍵を組み合わせて錠データを生成するステップとを実行するようにしている。

【００１６】

この構成においては、錠データがグループ・メンバの公開鍵で暗号化した錠データの秘密鍵の暗号文を含んでいるので、グループ・メンバのみによる暗号文の復号や署名を実現できる。

この構成において、上記秘密鍵を一方向性でない関数（逆関数がある関数）で上記秘密鍵を変形しこの変形秘密鍵を共通鍵で暗号化して保持するようにしてもよい。

また、グループ・メンバの公開鍵で共通鍵を暗号化するときにシード生成用の関数を用いてもよい。すなわち、グループ・メンバの公開鍵を所定の関数例えばハッシュ関数で演算し、このハッシュ関数の値と上記共通鍵との組み（所定の演算、ビット連結等）を当該グループ・メンバの公開鍵で暗号化する。このようにすると、グループ・メンバの公開鍵ごとに異なるシードが付け加わり、暗号化対象が変化するので、暗号文が複数あっても解読のヒントとなることが少ない。

【００１７】

また、この構成において、前記グループ・メンバは、個人、個人の集合、組織、組織の役職のいずれかとすることができる。

また、上記錠データを、上記錠データを単位として管理するようにしてもよい。利用者は、複数の錠データをあたかも錠の束を扱うように用いることができる。上記錠データはクライアントがアクセス可能なサーバに記憶しておくことができる。

【００１８】

また、上記錠データは、署名を検証するための公開鍵と、上記署名を行なうための署名用秘密鍵を変更権限所有者の公開鍵で暗号化した暗号化署名用秘密鍵と、上記錠データに含まれる所定のデータに対する上記署名用秘密鍵による署名とをさらに含むように構成してもよい。

【００１９】

また、この発明によれば、錠データを変更する方法において、第１の公開鍵と、上記第１の公開鍵に対応する秘密鍵を共通鍵で暗号化した暗号化秘密鍵と、上記共通鍵をグループ・メンバのそれぞれの公開鍵で暗号化した複数の暗号化共通鍵と、署名を検証するための第２の公開鍵と、上記署名を行なうための署名用秘

密鍵を変更権限所有者の公開鍵で暗号化した暗号化署名用秘密鍵と、上記第１の公開鍵、上記暗号化秘密鍵、上記暗号化共通鍵、上記第２の公開鍵および上記暗号化署名用秘密鍵に対して上記署名用秘密鍵を用いた行なった署名とを含んでなる錠データを記憶するステップと、上記錠データに含まれる上記暗号化署名用秘密鍵を上記変更権限所有者の秘密鍵で復号して署名用秘密鍵を生成するステップと、上記錠データを変更するステップと、変更した錠データに対して上記署名用秘密鍵で署名を行なうステップとを実行するようにしている。

【００２０】

この構成においては、錠データを生成した者を除けば、変更権限を有する者のみしか、署名用秘密鍵を取得できないので、変更後の錠データについて、署名が成功裏に検証された場合には、変更権限を有する者が錠データを変更したことを確認することができる。

【００２１】

また、この構成において、上記錠データを変更するステップを、上記第２の公開鍵を更新するステップと、上記署名用秘密鍵を更新するステップと、更新した署名用秘密鍵を上記変更権限所有者の公開鍵で暗号化して新たに生成した新たな暗号化署名用秘密鍵で、変更前の上記暗号化署名用秘密鍵を更新するステップと、上記更新後の署名用秘密鍵で署名を行なうステップとを含むように構成できる。この場合、変更権限所有者は、新たに署名用公開鍵、秘密鍵を設定することにより、変更権限所有者を設定することができる。

【００２２】

また、上記錠データは上記錠データのバージョンを示すバージョン識別子をふくんでもよい。また、上記錠データは、前バージョン扱い識別子を含み、この識別子に基づいて前のバージョンの錠データの取り扱いを制御するようにしてもよい。また、上記前バージョン扱い識別子が、上記錠データの変更内容に基づいて生成されるようにしてもよい。また、上記前バージョン扱い識別子は、上記錠データの変更の遡及的適用の有無を識別する情報を含んでもよい。

【００２３】

なお、この発明は、ハードウェアとして実現してもよく、また少なくとも一部

をソフトウェア実現態様で構成してもよい。また、ソフトウェア実現態様とする場合には、通信媒体やソフトウェアパッケージ（記録媒体）を利用してコンピュータ・システムにインストールすることができる。

【００２４】

【発明の実施の形態】

本発明の概要をまず述べる。以下の説明において個人の集合をグループと呼び、グループの要素、すなわち構成員である個人をメンバと呼ぶ。本発明は、公開鍵暗号方式において、グループの概念を導入したものである。すなわち、特定のグループに属する任意のメンバが復号可能である暗号化と、特定のグループに属する任意のメンバによる署名を代表的な機能とする暗号方式である。本発明では、グループ秘密鍵による署名を可能とすることにより、実際に署名したメンバを明確にせずグループ内のメンバによる署名であることのみを明らかにできるという利点を有する。

【００２５】

グループに対応する秘密鍵と公開鍵のペアを提供し、それぞれをグループ秘密鍵、グループ公開鍵と呼ぶ。さらにグループ暗号鍵を暗号化する共通鍵（慣用暗号鍵）を提供する。グループ秘密鍵を共通鍵で暗号化し、この共通鍵をすべてのメンバの個人公開鍵でそれぞれ暗号化し、その暗号化された共通鍵の集合を作る。この暗号化された共通鍵の集合および暗号化したグループ秘密鍵は、少なくとも各メンバが入手可能なものとしておく。これにより、グループ内の任意のメンバは、自分自身の個人秘密鍵を用いて、対応する個人公開鍵で暗号化された共通鍵を復号することができ、さらに、この共通鍵でグループ秘密鍵を復号すること、すなわち獲得することができる。よって、グループ公開鍵で任意の情報を暗号化すれば、グループのメンバは、その暗号化された情報を上記の手法で獲得したグループ秘密鍵を使用して復号することができる。同様に、グループのメンバは、グループ秘密鍵を使用して署名を行うことができる。

【００２６】

以下では、これらの機能を実現するために必要となるグループ秘密鍵およびグループ公開鍵のペアの生成、共通鍵の生成、グループ公開鍵による暗号化処理、

グループ秘密鍵による復号処理、さらにグループのメンバの追加、削除等の変更の際の処理について明らかにする。

【００２７】

情報の暗号化により、情報の機密性を保持しようとする場合には、暗号化された情報自体の所在は問わない、すなわち明らかにされない。このことは、一旦、暗号化された情報を、何らかの理由により、暗号化し直さなければならない機構は受け入れがたいことを意味する。なぜなら、所在を問わないということは、暗号化し直さなければならない情報の所在の特定が困難であるからである。そのため、本発明ではグループの構成員であるメンバに変更があった場合は、一旦、暗号化された情報の再暗号化ではなく、鍵の作り直しで対応することになる。従来の個人を単位とする公開鍵暗号方式では、恒久的な存在である個人と鍵が１体１対応であり、鍵の作り直しという要請はなかったが、本発明では、グループ対鍵という対応関係が発生し、グループの構成要素の変更に基づく鍵の変更要請が発生する。

【００２８】

本発明の暗号および署名方式は、上述のグループ単位の暗号化および署名のみではなく、組織内の特定の役割を果たすポジションにある個人、例えば企業内の人事部長といった役割に対応する鍵を提供する場合にも有効な機能を持つ。例えば、人事部長の役割に対応する鍵があり、人事部長を努める個人が変更された場合には、人事部長という役割に対応する鍵を変更することによって実世界の変更に対応可能である。人事部長に対して暗号化文書を送付する側は、従来からの当該役割（人事部長）に対応する公開鍵を使用して情報を暗号化すればよい。また、新たな人事部長は、すでに暗号化されている情報を変更することなく、過去に当該役割に対応する公開鍵を使用して暗号化された情報を参照することが可能となる。

【００２９】

企業内のプロジェクト等ある目的を有するグループにおいては、複数人による協同作業や役割に基づいた作業が重要であり、その協同作業グループのメンバや、役割を果たす個人は固定的なものではない。従って、グループの中と外との機

密性保持能力はより高度なものが要求される。

【００３０】

また、情報ネットワークサービスにおいて公証局と呼ばれる公開鍵に対する所定レベルの保証を与えるシステムが利用されつつあるが、本発明においては、公証局を利用することによって無効となった鍵の排除が可能である。

【００３１】

次に、本発明を構成する各要素について説明する。説明は以下の項目について行う。

（１）複合錠

（２）グループ錠

（３）個人錠

（４）個人錠の秘密鍵

（５）複合錠リスト

（６）信用体

（７）公証局

【００３２】

（１）複合錠

複合錠は、次に説明するグループ錠（役割錠）、個人錠を実現する錠の総称であり、具体的には以下の要素を持つ電子データである。

【００３３】

ａ．名前

複合錠に対応する実世界の実態を意味する人間が可読な文字列であり、複合錠の識別子としての役割を有する。人間が異なる文字列を同一と誤って判断することを防ぐためスペースあるいは混同されやすい文字列の使用はしないことが好ましい。

【００３４】

ｂ．作成日時、作成者

複合錠を作成した日時、および複合錠の作成者である。作成者は、作成した複合錠全体に対する署名を行う。署名の手順には、複合錠を構成する電子データを

作成者の個人鍵で暗号化することが含まれる。

ｃ．共通鍵で暗号化した秘密鍵

復号錠の秘密鍵を共通鍵で暗号化したものである。

【００３５】

ｄ．共通鍵のリスト

複合錠の秘密鍵を暗号化した共通鍵を、メンバの公開鍵で暗号化し、メンバの名前（メンバを識別するデータであればよい）をラベルとして付与したもののリストである。メンバの秘密鍵によって復号することにより、共通鍵を復号でき、この結果、さらに複合錠の秘密鍵を復号して獲得できる。複合錠の秘密鍵を用いて他から送付された暗号の復号が可能である。

【００３６】

ｅ．公開鍵

複合錠の公開鍵である。情報を暗号化する際には、この公開鍵によってデータ変換を実行し、暗号とする。

【００３７】

ｆ．変更錠の秘密錠リスト

情報の機密性保持等に用いる公開鍵と秘密鍵のペアとは独立に、複合錠の変更権を制御するための公開鍵と秘密鍵とのペアが必要となる。このペアを変更錠と呼ぶ。この変更錠の秘密鍵を、変更権所有者の公開鍵で暗号化し、変更権所有者の名前をラベルとして付与したもののリストを複合錠は保持する。複合錠の変更権所有者のみが、その複合錠の変更、例えば、メンバの追加、削除等を行い新しいバージョンの複合錠を作成することが許される。この変更権所有者は予め指定される。ある複合錠が変更権所有者によって変更され、新しいバージョンとなったときは、旧バージョンの錠を信用している人は、新バージョンの錠を自動的に信用するように設定できる。これを自動信用機構と呼ぶ。錠の信用については後述する。正当な変更権所有者によって複合錠の変更が行われたことを明確にするために、変更に際しては、変更錠の秘密鍵による署名を行う。ただし、複合錠のメンバ全員がその複合錠の変更権を有する場合には、機密保持用のペアを用いる。この場合には、現バージョンの秘密鍵による署名を行う。

【００３８】

ｇ．変更錠の公開鍵

上述の変更錠の秘密鍵とペアを構成するものであり、上記の変更錠の秘密鍵による署名された複合錠の復号等に使用され、署名の確認が可能となる。なお、以上に加えて複合錠の有効期限や公証局と交信できないオフライン期間における有効期間を付加し、複合錠の利用を制御するようにしてもよい。

【００３９】

（２）グループ錠

グループ錠とは、実世界のグループに対応する複合錠である。グループは一般に複数のメンバを含む。役割錠（例えば人事部長の役割）としても機能する。

【００４０】

（３）個人錠

個人錠は、個人に対応する複合錠である。個人錠も複合錠により実現される。個人錠としての複合錠のメンバは、供託者を指定する。供託者とは、その個人以外の人に対して条件付きでその個人と同一の権利が与えられた人のことである。これは、その個人がパスフレーズを忘れた場合等、その個人の代理者としての役割を果たしうる人を供託者として情報の復号を可能とする。これは、例えば企業内での情報の機密性、および復号可能性を１人の個人に託する危険性を考慮したものである。また、情報の監査や検閲を行うために用いることも可能である。供託者が個人錠を利用することができる条件として複数の指定された供託者の承認を必要とするといった設定も可能である

【００４１】

（４）個人錠の秘密鍵

個人錠の秘密鍵は、利用者のみがアクセスできるように守られている。例えば、個人（利用者）のみが知っているパスフレーズを暗号／復号の鍵として使った共通鍵暗号手法により、秘密鍵を守ることができる。もしくは、利用者が常に携帯できる特殊な器具（ＩＣカード、ＰＤＡ：パーソナルデジタルアシスト等）に個人錠の秘密鍵を記憶させて、必要なときに取出すようにしてもよい。また、利用者の身体／肉体的特徴（指紋、声紋、眼底網膜パターン等）を検出してアクセ

スできるようにしてもよい。署名による特徴検出などを利用してもよい。その他種々のアクセス制御手法を用いることができる。このようにして、利用者のみが、秘密鍵を必要になった時点でその秘密鍵を入手できる。

【００４２】

（５）複合錠リスト

個人が所有する信用度が明確な複合錠リストである。複合錠とその対応する信用度がペアとして保持される。複合錠を利用するときは、このリスト中の信用度により判断される。ここに存在しない複合錠の信用度は不明であると解釈される。例えば、暗号文の復号を許容する個人またはグループをこの複合錠リストで指定し、対応する複合錠からその公開鍵を取得して暗号化秘密鍵を生成する際に用いられる。すなわち、この複合錠のリストは信用した個人やグループの公開鍵を間接的に登録した公開錠リストであり、個人やグループの公開鍵を直接登録するものであってよい。なお、複合錠そのものは、装置に記憶されたもの以外に、遠隔に位置する装置に記憶されたものを参照するものでもよく、装置内および装置外に記憶された複合錠を混在して用いるものであってもよい。

【００４３】

（６）信用体

本発明におけるグループにおいて使用される複合錠は、誰でも生成できるが、信用されないと有効な錠とは成り得ない。複合錠を信用するとは、実世界の実態として存在するグループ（役割を含む）と、そのグループに対応するであろう複合錠とが実際に対応することを信用するという意味である。具体的には、単にグループと複合錠とが対応するだけではなく、信用する時点での実世界のグループのメンバと複合錠に含まれるメンバとが一致しなければならない。例えば「人事部人事１課」という名称の複合錠があったとする。「人事部人事課」という実世界のグループは存在するが、「人事部人事１課」という実世界のグループは存在しないかもしれない。「人事部人事１課」という実世界のグループが存在したとしても、それに対応する正当な複合錠は存在していないかもしれない。よって複合錠の名称のみを根拠に複合錠を信用することはできない。また、「人事部人事１課」内のメンバが変更されたにもかかわらず複合錠のメンバ中に過去のメンバ

が残っているような場合には信用することができない。

【００４４】

どの複合錠が信用できるかについての情報を信用情報という。また、信用情報自体の信用度を示す情報も信用情報である。信用情報を保持する主体を信用体という。信用情報、および複合錠を何を根拠として信用するのかは信用体の任意である。信用体には、個人と以下の（７）で説明する公証局の２種類が存在する。信用体は他の信用体を信用することができる。このとき信用される信用体を被信用体と呼ぶ。信用体は、複合錠を信用しているときにのみ、この複合錠を利用することになる。信用体がその複合錠に対する直接の信用情報を持たない場合は、信用している信用体がその複合錠を信用している場合には信用する。とすることが可能である。

【００４５】

例えば、個人「田中さん」および公証局「Ｘ商事」がいずれも信用体であるとき、個人「田中さん」が公証局「Ｘ商事」を信用しているとき、公証局「Ｘ商事」が信用しているものは、個人「田中さん」は自動的に信用する。しかし、逆に個人「田中さん」が信用しているものを公証局「Ｘ商事」が信用するとは限らない。という関係である。

【００４６】

信用の程度には種類があり、信用レベルと呼ばれる。この信用レベルを使用して信用度の未知の複合錠の信用度を演算によって求めることが可能である。このとき使用される信用レベルは、例えば以下の表の信用レベルである。

【００４７】

【表１】

レベル◎：完全に信用する（ｅｘ．自分自身）。

レベル○：十分に信用する。

レベル△：ある程度信用する。

レベル？：不明。

レベル×：信用しない。

【００４８】

信用レベルが未知の複合錠に対する信用レベルを同一の複合錠に対する独立した異なる２つの信用体、例えば２人の個人Ａ、Ｂの有するその複合錠に対する信用レベルから求める場合の例を図１に示す。図１の第１行は個人Ａ、左端列は個人Ｂの信用レベルを示すもので、それぞれの場合についての結果が表として示されている。例えば個人Ａの設定した信用レベルが○であり、Ｂが設定した信用レベルが？である複合錠の信用レベルは○となる。

【００４９】

また、信用体に対する信用レベルと、その信用体の他の信用体への信用レベルまたは複合錠への信用レベルを使用した信用レベルの演算には、例えば図２に示すような演算規則が使用される。図２の第１行は信用体に対する信用レベル、左端列はその信用体の他の信用体への信用レベルまたは複合錠への信用レベルを示すもので、それぞれの場合についての結果が表として示されている。例えばその信用体の信用レベルが○であり、その信用体が設定した信用レベルが？である複合錠の信用レベルは？となる。このような図１あるいは図２で示す演算規則を用いて信用度が未知の信用体あるいは複合錠の信用度を決定することが可能である。

【００５０】

（７）公証局

公証局は、上述のように信用体の１つである。公証局の提供する機能は、例えばある暗号システムが使用されている企業や組織といった単位での公の信用を表現、提供することである。公証局における複合錠の信用基準は、当該公証局を運営する企業や組織が任意に決定する。この信用基準の決定方式には、次に述べるようないくつかの方式が考えられる。以下の説明において「保証する」とは、登録されようとする複合錠が正当であることを登録者以外の個人が証明する行為をいう。

【００５１】

ａ）公証局の特定の管理者による何らかの手続により正当であることを確認する。確認がなされた場合に、公証局がその複合錠を信用する。ここで何らかの手続とは、実世界における任意の手続である。例えば申請用紙に捺印がおされてい

ること、あるいは、申請者の身分証明書の確認手続による等である。この他、名前の重複確認、登録者毎に指定されている他の特定の個人による保証、予め決められた人数以上の保証、または、公証局の信用している個人の署名が予め決められた人数以上の場合等に信用して登録するようにしてもよい。

【００５２】

【実施例】

以下、グループ錠を用いた暗号方式の実施例を示す。なお、ここでは、上述の説明における複合錠の中のグループ錠を取り上げて説明するが、複合錠のもう１つの種類である個人錠においても、グループ錠におけるメンバが供託者に変更になる他は、同様の構成、手続で暗号方式が構成される。また、グループ錠の特殊な用途として上述した役割錠があるが、グループ錠を役割錠として機能させるためには、グループ錠の構成メンバ数を１とし、その唯一のメンバとして、現在その役割を果たしている個人とすればよい。ただし、副社長の役割錠のメンバに副社長自身の他にその秘書を含めるといった運用も可能である。

【００５３】

本発明の暗号方式を利用する各人は２つの錠リストを有する。すなわち、ａ）各人が信用しているグループ錠および個人錠のリストである「公開錠リスト」、および、ｂ）各人が自身の秘密鍵を元に直接もしくは間接に秘密鍵を獲得できるグループ錠のリストである「秘密錠リスト」である。ここでは、簡単のために、「公開錠リスト」に含まれているグループおよび個人錠は信用しているものとし、「やや信用している」といった中程度の信用を与えることはしない。また、信用するか否かは、上述の信用程度の演算規則を用いたものあるいは利用者の判断等に基づくものとし、以下の実施例中での詳細な説明は省略する。ただし、グループ錠を変更した際に、直前のグループ錠を信用している場合における自動信用機構、すなわち変更前のグループ錠を信用している場合は、変更後のグループ錠を自動的に信用するものとする。また、上述の公証局への登録手続についても以下の実施例中では直接触れないが、上述した説明のようにネットワーク中に公証局がある場合には、生成、あるいは変更された錠については、公証局への登録がなされる。ただし、この登録手続は、本発明の必須要件ではない。

【００５４】

まず、この実施例の全体構成を図３により説明する。本実施例の基本的な機能は、個人対個人で、情報を正確に機密性を保持して伝達することである。ただし、個人は、グループに所属していることもある。情報の伝達は、メールのような直接伝送する方法でも、ファイルサービスを介した間接的な方法でも良い。

【００５５】

図３に示すように個人間で伝達するものは、暗号だけでなく、必要に応じて個人公開鍵や、グループ錠も伝達する。個人公開鍵やグループ錠はともに、それが実世界に実在する個人やグループとの正しい対応関係にあるか否かの判断を必要とする場合には、その判断手続を確立することが必要となる。

【００５６】

図３に示す「個人」における平文から暗号への暗号化の際には、復号可能とすべき個人やグループを自身が保持する錠に対応する錠を錠リストから選択して、暗号化する。これにより、選択した個人や、選択したグループに属する個人が復号可能な暗号が生成される。または、共通鍵ＫＡによって平文を暗号化するとともに、この暗号の復号に必要な復号鍵ＫＢを復号可能とすべき個人やグループを自身が保持する錠に対応する錠を錠リストから選択して、暗号化し、これらを送付する。

【００５７】

伝達された暗号化情報を復号する際には、得られた暗号が自身の個人秘密鍵によって直接復号可能であれば、自身の個人秘密鍵を用いて復号する。自身が間接もしくは直接に属するグループによって復号可能であれば、自身の個人秘密鍵を用いてグループ錠をグループ秘密鍵に変換することでグループ秘密鍵を獲得し、それを用いて復号する。グループ秘密鍵は利用後直ちに捨て、単独では保持しない。本方式において、「個人」に秘密遵守を要請されるのは、個人秘密鍵だけである。共通鍵ＫＡによって暗号化が実行された場合には、まず、復号に必要な復号鍵ＫＢを自身の個人秘密鍵を用いて復号する。自身が間接もしくは直接に属するグループによって復号可能であれば、自身の個人秘密鍵を用いてグループ錠をグループ秘密鍵に変換することでグループ秘密鍵を獲得し、それを用いて復号鍵

ＫＢを獲得し、この復号鍵ＫＢによって平文を復号する。

【００５８】

［グループ錠］

本実施例におけるグループ錠の構造を図４に示す。図４における各記号の説明を次に示す。

【００５９】

L_G：このグループ錠のラベル

文字列である。ある個人の錠リストの中では重複を許さない。全体としては重複は生じうるので、識別子として利用することはしない。ただし、ラベルが一致しなければ公開鍵も一致しないため、そのことを利用して処理を高速化することはできる。

【００６０】

P_G：このグループ錠の公開鍵

利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。このグループに直接もしくは間接に属するすべての個人に復号可能な暗号化を行う際には、この公開鍵を用いて暗号化する。また、このグループに直接もしくは間接に属する任意の個人として署名されたものを確認する際には、この公開鍵を用いて署名の確認を行う。公開鍵はグループ錠の中に、そのままの形式で含まれており、誰でもが参照できる。

【００６１】

S_G：このグループ錠の秘密鍵

利用する公開鍵暗号システムに応じた秘密鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。対応する公開鍵で暗号化された暗号を復号する際に用いる。また、このグループに直接もしくは間接に属する任意の個人として署名する際にも用いる。この秘密鍵は、直接もしくは間接的に個人の秘密鍵および共通鍵により複合的に暗号化されており、利用する際には、個人の秘密鍵を用いてまず共通鍵を復号し、その後グループ錠の秘密鍵を復号して獲得し、利用後はすぐに捨て去り、単独で保持することはしない。

【００６２】

C_G：グループ上の秘密鍵を暗号化する共通鍵

従来の共通鍵であり、ＤＥＳやＦＥＡＬ等、周知のものを用いることができる。鍵の大きさは一般に４０ビットから１２８ビットである。

【００６３】

C_G（S_G）：共通鍵C_Gで暗号化されたグループ錠の秘密鍵

グループ錠の秘密鍵S_Gを共通鍵C_Gで暗号化した暗号文である。秘密鍵S_Gを取得するには共通鍵C_Gが必要となる。

【００６４】

Ｍｉ：このグループのメンバ

概念上の存在であり、データ構造には直接現れない。メンバには個人およびグループがなり得る。なお、前述のようにグループ錠ではなく個人錠の場合には、このメンバは供託者となる。

【００６５】

P_U：このグループ錠変更用の公開鍵

利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。グループはメンバの追加もしくは削除といった変更を行う必要がある。その変更を行える権利を持つ人を識別する方法として、専用の公開鍵と秘密鍵の対を利用する。これはその公開鍵である。グループ錠には、変更用の秘密鍵が、変更権を所有する個人の個人秘密鍵により直接もしくは間接に暗号化されて含まれている。グループ錠を変更したときには、新しいグループ錠をその変更用秘密鍵により署名する。変更用秘密鍵は変更権の所有者でなければ入手できないため、その署名が確認できれば正当な変更権の所有者による変更であることが確認できる。この確認処理は、以前のグループ錠を信用していれば自動的に行うことができる。この変更用公開鍵は、そのままの形式で含まれているため誰でも参照できる。

【００６６】

S_U：このグループ錠変更用の秘密鍵

利用する公開鍵暗号システムに応じた秘密鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。機能は、P_Uの説明に記載のと

おりである。

C_U：グループ錠変更用の秘密鍵S_Uを暗号化する共通鍵

従来の共通鍵であり、ＤＥＳやＦＥＡＬ等、周知のものを用いることができる。鍵の大きさは一般に４０ビットから１２８ビットである。

C_U（S_U）：共通鍵C_Uで暗号化されたグループ錠変更用の秘密鍵

グループ錠変更用の秘密鍵S_Uを共通鍵S_Uで暗号化した暗号文である。秘密鍵S_Uを取得するには共通鍵C_Uが必要となる。

【００６７】

Ｖ：このグループ錠のバージョン番号

自然数である。新規にグループ錠を生成したときには、１となる。グループ錠のバージョンを示す。変更するとバージョン番号は基準となったバージョンより１多い数とする。

【００６８】

Ｆ：直前のバージョンの扱いを示す値

「不要」、「必要」、「抹消」のいずれかの値を取る。グループ錠の変更を行った際、直前のバージョンを持つ個人は、新しいバージョンを入手することにより直前のバージョンを適切に扱う必要がある。「不要」は、直前のバージョンが不要となることを意味する。「必要」は、直前のバージョンにより作られた暗号を復号するため、直前のバージョンによりなされた署名を確認するために必要である。この場合には、新たに暗号化や署名を行うときには最新のバージョンを使わなければならない。「抹消」は、「必要」に近いが、自身が新しいバージョンの秘密鍵を獲得できない場合には、直前のバージョンを削除しなければならないことを意味する。新規にグループ錠を生成したときには、この値は意味を持たない。

【００６９】

Ｕｉこのグループの変更権所有者

概念上の存在であり、データ構造には直接現れない。変更権所有者には、個人およびグループを指定できる。

【００７０】

L_{Mi}：Ｍｉのラベル

文字列である。このグループ錠の直接のメンバである、他のグループ錠もしくは個人公開鍵のラベルである。個人錠については、本実施例においては明記しないが、対応する個人が管理する秘密鍵と、公開する公開鍵とからなり、少なくとも公開鍵にはラベルが付与されているとする。

【００７１】

P_{Mi}：Ｍｉの公開鍵

利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。このグループの直接のメンバの公開鍵である。

【００７２】

P_{Mi}（C_G）：P_{Mi}で暗号化されたC_G

利用する公開鍵暗号システムに応じた暗号処理により、C_Gを暗号化した結果である。これを用いてC_Gを獲得するためには、P_{Mi}に対応する秘密鍵ＳＭｉが必要である。これは、対応するL_{Mi}をインデックスとした配列により保持する。

【００７３】

L_{Ui}：Ｕｉのラベル

文字列である。このグループ錠の変更権所有者である個人の個人錠のラベルである。

【００７４】

P_{Ui}：Ｕｉの公開鍵

利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。このグループ錠の変更権所有者である個人の公開鍵もしくはグループ錠の公開鍵である。

【００７５】

P_{Ui}（C_U）：Ｕｉの公開鍵で暗号化されたC_U

利用する公開鍵暗号システムに応じた暗号処理により、C_Uを暗号化した結果である。これを用いてC_Uを獲得するためには、P_{Ui}に対応する秘密鍵S_{Ui}が必要である。これは、対応するL_{Ui}をインデックスとした配列により保持する。な

お、本実施例では、パケット通信におけるパケットのデータ構造のように、秘密鍵に対してデータを識別するための情報を付加した上で暗号化を行う。従って、この暗号化秘密鍵を復号した際に付加的情報に基づいて秘密鍵が正常に復号されたか否かを容易に判別することができる。

【００７６】

Ｓｉｇ（S_U）：全体に対するS_Uによる署名

署名を示すデータ列である。ここで全体とは、L_G、P_G、C_G（S_G）、Ｖ、Ｆ、P_U、C_U（S_U）、L_{Mi}、P_{Mi}（C_G）、L_{Ui}、P_{Ui}（C_U）である。署名とは、秘密鍵S_Uによる暗号化処理である。公開鍵暗号システムでは、通常と逆に、秘密鍵により暗号化し、それを公開鍵で復号することができる。公開鍵で復号できるには、秘密鍵により暗号化しなければならないため、公開鍵で復号できることを確認することにより、秘密鍵により署名されたことを確認できる。実際には、メッセージダイジェストをその対象範囲に対して行い、その処理結果に対して、秘密鍵S_Uにより署名する。メッセージダイジェストとは、署名の対象範囲を全て暗号化するにはコストがかかるために、対象範囲のデータサイズには独立に、対象範囲の内容に応じて１２８ビット程度の情報を生成する処理である。メッセージダイジェスト処理アルゴリズムは公開されたものを用い、鍵も利用しない。よって確認の際には、対象データをメッセージダイジェストし、署名を復号した結果と一致するか否かを確認することになる。メッセージダイジェストの処理は、チェックサムに類似した処理であるが、処理過程において一方方向関数を用いることにより、同じ結果を生成する入力データを偽造することを困難にしている。また、生成されるデータサイズが大きいため、総当たり的な入力データの偽造も困難である。「メッセージダイジェスト」という名称は、暗号関連においては一般的な名称であり、良く知られた方式である。Ｓｉｇ（S_U）はメッセージダイジェスト処理関数をf_{md}とし、対象とするデータの複合操作を算術和で表現するとし、S_Uを用いた署名を関数S_Uで表現するとすると、次の処理を施した結果となる。

【００７７】

【数１】

$$S_U(f_{md}(L_G+P_G+C_G(S_G)+P_U+C_U(S_U)+\sum_{i=1}^{n}(L_{Mi}+P_{Mi}(S_G)+L_{Ui}+P_{Ui}(S_U))))$$

【００７８】

S_U'：前バージョンのS_U

利用する公開鍵暗号システムに応じた秘密鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。直前のバージョンの変更用秘密鍵である。機能は、S_Uと同様である（詳細は、P_Uの説明参照）。

【００７９】

$Sig(S_U')$：全体に対するS_U'による署名

署名を示すデータ列である。ここで全体とは、L_G、P_G、$C_G(S_G)$、V、F、P_U、$C_U(S_U)$、L_{Mi}、$P_{Mi}(C_G)$、L_{Ui}、$P_{Ui}(C_U)$、$Sig(S_U)$である。これは、新規に作成された場合には、付与されない。$Sig(S_U)$と同様に表記すると、次のように表せる。

【００８０】

【数２】

$$S_U(f_{md}(L_G+P_G+C_G(S_G)+P_U+C_U(S_U)+\sum_{i=1}^{n}(L_{Mi}+P_{Mi}(C_G)+L_{Ui}+P_{Ui}(C_U)+Sig(S_U))))$$

【００８１】

なお、本実施例ではデータ全体に対して署名を行うようにしたが、改竄を防ぎたい一部データに対して署名を行うようにしてもよい。

【００８２】

[公開錠リスト]

図５に本実施例における公開錠リストの構造を示す。公開錠リストとは各個人が独立に所有するもので、その個人が信用しているグループ錠および個人錠を、その錠のラベルをインデックスとした配列で保持するものである。

【００８３】

図５に示すように、公開錠リストは、Ｇｉ：信用しているグループ錠、L_{Gi}：グループ錠Ｇｉのラベル、Ｉｉ：信用している個人の公開鍵、ＬＩｉ：個人の公開鍵Ｉｉに対応するラベルから構成される。

【００８４】

公開錠リストへの新たなデータの追加の際に必要な錠の信用は、本実施例においては公開錠リストの所有者の判断に任されるものとする。ただし、既に信用しているグループ錠の次バージョンの自動信用は行うこととする。前述の信用レベルに関する演算規則を用いて信用できる錠あるいは信用体を決定することも可能である。この場合前述の公証局に登録された信用関係を利用することにより確実かつ容易に信用レベルを求めることが可能となる。

【００８５】

暗号化の際に、復号可能なグループおよび個人を指定するが、それは対応するグループ錠もしくは個人錠を１個以上、この公開錠リストから選択することにより指定する。

【００８６】

署名の正当性を確認する際には、署名時に用いられた秘密鍵に対応する公開鍵をこの公開錠リストから取り出して利用する。

【００８７】

[秘密錠リスト]

図６に本実施例における秘密錠リストの構造を示す。秘密錠リストとは各個人が独立に所有するもので、その個人が秘密鍵を獲得できるグループ錠を、そのグループ錠のラベルをインデックスとした配列で保持するものである。秘密鍵の獲得は、その個人の個人秘密鍵を、グループ錠に直接もしくは間接に適用することにより行われる。

【００８８】

図６に示すように、秘密錠リストは、Ｇｉ：秘密鍵が利用可能なグループ錠、、L_{Gi}：グループ錠Ｇｉのラベルから構成される。

【００８９】

秘密錠リストへの追加は、公開錠リストへのグループ錠の追加処理の中で、自身の個人秘密鍵を直接もしくは間接に適用することによりそのグループ錠内部のグループ秘密鍵を獲得可能であるならば追加することにより行う。よって利用者は追加処理を意識する必要はない。自身の個人秘密鍵により、そのグループ錠内部のグループ秘密鍵が獲得できるからといって、そのグループ錠を信用する根拠にはならないことには注意が必要である。

【００９０】

復号の際に、復号可能性の判断を秘密錠リストを用いることにより高速化する。また、実際の復号処理においても、必要なグループ秘密鍵の獲得処理にこの秘密錠リストを利用する。

【００９１】

署名の際には、自身の個人秘密鍵を用いる以外にも、この秘密錠リスト中のグループ秘密鍵を用いて署名することができる。このようにすれば、暗号文の受け手側で送り手の個人やグループを識別することができる。また、署名とともに署名に用いた秘密錠の公開鍵を添付すると署名の確認が容易になるとともに、署名を確認することなく公開鍵のみで送り手を容易に確認することができる。

【００９２】

［暗号］

本実施例における暗号の構造を図７に示す。本実施例においては、グループ錠のL_{Mi}とP_{Mi}（S_G）のペアのリストと同様の構造を持たせることにより、複数の秘密鍵のいずれかを用いることにより復号可能としている。これにより、複数人に開示したい情報を暗号化する際に、必ずしもグループ錠を作成する必要をなくしている。すなわち、公開錠リストから任意に選択した個人やグループで構成される受け手のグループを一時的に作成することができる。

【００９３】

図７中の各記号の意味を以下に説明する。

Ｐｉ：復号できるグループ錠もしくは個人の公開鍵

利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。

【００９４】

Ｌｉ：Ｐｉのラベル

文字列である。

【００９５】

Ｄ：平文（機密を保持すべき情報）

任意のデータ列である。

【００９６】

Ｋ：平文Ｄを暗号化した共通鍵

公開鍵暗号は、暗号化処理および復号処理が遅いため、共通鍵暗号で平文を暗号化し、その共通鍵のみを公開鍵暗号により暗号化するハイブリッド方式を採用することが一般的である。このＫは、その共通鍵である。本実施例においては、ＫをＰｉでそれぞれＰｉで暗号化することにより、複数のグループもしくは個人による復号を可能とする。

【００９７】

Ｐｉ（Ｋ）：Ｐｉで暗号化したＫ

Ｋ（Ｄ）：で暗号化したＤ

【００９８】

Ｓ：暗号化処理を行った人が利用可能な秘密鍵

暗号に署名を付与する際に用いる、秘密鍵である。自身の個人秘密鍵か、秘密鋌リストに含まれているグループ鋌の秘密鍵のうちの１つを用いる。

【００９９】

Ｐ：署名に用いた秘密鍵Ｓと対になる公開鍵Ｐ

署名の確認の際には、署名者が署名に用いたと主張する秘密鍵に対応する公開鍵を利用する。その公開鍵を特定するために保持する。暗号文の受け手側においてその公開鍵が自身の公開鋌リストに含まれていれば、自身が信用しているグループもしくは個人により署名されていることを確認することができ、暗号文の発信者または発信したグループを確認することができる。

【０１００】

Ｓｉｇ（Ｓ）：全体に対するＳによる署名

署名を示すデータ列である。ここで全体とは、Ｌｉ、Ｐｉ（Ｋ）、Ｋ（Ｄ）である。署名に関しては、グループ鍵の構造のＳｉｇ（S_U）の項を参照。同様の表記に従えば、Ｓｉｇ（Ｓ）は次のように表せるものである。

【０１０１】

【数３】

$$S\left(f_{md}\left(\sum_{i=1}^{n}\left(Li+Pi\left(K\right)\right)D\right)\right)$$

【０１０２】

［処理の流れ］

本実施例の具体的な処理の流れを以下、図８から図１６に示されるフローチャートによって説明する。

【０１０３】

［グループ鍵生成］

グループ鍵生成についてのフローを図８に示す。グループを作成するとき（追加変更するときも同様）には、新しく指定するメンバに対応するグループ鍵もしくは個人の公開鍵は作成者が信用している必要がある。そのため、新しく指定するメンバのグループ鍵もしくは個人の公開鍵を信用していないときには、グループ鍵の作成に先立って、信用すること、すなわち鍵リストへの追加を行わなければならない。

【０１０４】

作成したグループ鍵は、まず自身の鍵リストに追加される。鍵リストとは、公開鍵リストと秘密鍵リストの総称である。さらに必要な者（作成したグループ向けに暗号化された暗号を復号する際に、グループのメンバはこのグループ鍵が必要である。逆にこのグループ向けに暗号化する際にもグループ鍵が必要となる。暗号化は任意の人が行える。そのためメンバおよびこのグループ向けの暗号化を行う可能性のある人への配布が必要となる）へ配布する。離れたセンタで保管し、暗号文の送り手や受け手の必要に応じて複合鍵を送ったり、複合鍵の必要な情報のみを送るようにしてもよい。本実施例においては、配布機構の説明は省略す

る。

【０１０５】

図８のフローについて詳細に説明する。まずステップ１０１において生成するグループ錠のラベルを入力する。ステップ１０２では、入力されたラベルと同じラベルの錠がすでに錠リスト中にあるかが検討される。重複するラベルの錠の作成は拒否されることになり、すでに錠リスト中に同じラベルのものがある場合はステップ１１３に進みグループ錠の作成が中止される。同じラベルのものが無い場合は、ステップ１０３に進む。

【０１０６】

ステップ１０３およびステップ１０４では、メンバＭｉと変更権所有者Ｕｉが指定される。メンバは、このグループ錠を使用した暗号システムを利用するメンバであり、変更権所有者は、このグループ錠の変更、例えばメンバの追加、削除等を行う権利を有する者である。メンバ、および変更権所有者は、いずれも個人に限らずグループでの登録が可能であり、グループ錠生成者が有する公開錠リストの中から１つ以上のグループ錠もしくは個人の公開鍵を選択して指定される。

【０１０７】

ステップ１０５では、生成されるグループ錠の秘密鍵S_G、公開鍵P_Gおよび共通鍵C_Gを生成する。ステップ１０６では、生成された秘密鍵S_Gを共通鍵ＣＧで暗号化してC_G（S_G）を生成する。さらに、この共通鍵C_GをメンバＭｉのそれぞれの公開鍵P_{Mi}で暗号化したP_{Mi}（C_G）を生成し、それぞれにラベルL_{Mi}を対応させる。

【０１０８】

ステップ１０７では、生成するグループ錠の変更用秘密鍵S_U、変更用公開鍵P_Uおよび変更用共通鍵C_Uが生成される。ステップ１０８では、生成されたグループ錠変更用秘密鍵S_Uを共通鍵C_Uで暗号化し、C_U（S_U）を生成する。そして共通鍵C_Uを変更権所有者の公開鍵P_{Ui}によって暗号化し、P_{Ui}（C_U）を生成し、それぞれにラベルL_{Ui}を対応させる。

【０１０９】

ステップ１０９では、生成されるグループ錠のバージョン番号を設定する。ス

テップ１１０では、それぞれのステップで生成された、L_G，P_G，C_G（S_G），P_U，C_U（S_U），V，P_{Mi}（C_G），P_{Ui}（C_U）の各データを一体とする。ステップ１１１では、一体となった前データに対する変更用秘密鍵S_Uによる署名、すなわちデータ変換が実行される。ステップ１１２でグループ錠生成者の錠リストにグループ錠を登録追加することでグループ錠の生成が終了する。生成されたグループ錠は先に説明した図４に示す構成を有する。

【０１１０】

［錠リストへの追加］

図９に錠リストへの追加手続のフローを示す。錠リストへの追加は、信用できるグループ錠もしくは個人の公開鍵だけについて行われる。この処理は、自身が生成および変更（新しいバージョンの作成）したグループ錠の追加、他者から得たグループ錠の追加のいずれにおいても用いられる。

【０１１１】

本実施例では、公証局を用いて鍵を配布したり、電子メールやフロッピを介して鍵を配布したりという配布に関する処理は含めていない。また、鍵に対する署名を利用し、その署名者に対する信頼度、署名者の鍵に対する信用度の演算を行い、鍵の信用度を算出するような処理は省略してある。前述した信用度の演算による信用度レベルの獲得をこのフロー中に含め、信用度の判断に用いることは可能である。本実施例においては、既に信用しているグループ錠の新しいバージョンの自動的な信用手続きについては示してある。ここでは、新しいバージョンが、直前のバージョンの変更用秘密鍵によって署名されていることが確認できた場合にのみ自動的に信用している。

【０１１２】

秘密錠リストへの追加は、信用できたグループ錠の中から、自身の個人秘密鍵を用いることにより直接もしくは間接に、そのグループ錠の秘密鍵を獲得できるものだけを追加する。

【０１１３】

図９に示すフローを詳細に説明する。ステップ２０１で追加する錠の指定が行われると、ステップ２０２，２０３，２０４において、直前のバージョンの錠の

変更用秘密鍵S_U'による署名の有無、信用の有無、署名の正確性について判断され、いずれかが「いいえ」の場合に、ステップ２１４に進み、追加する錠を信用するか否かを、信用錠の所有者自身が判断して入力する。信用する場合は、ステップ２１０に進み、信用しない場合は、錠リストへの追加は実行しない。ステップ２１４および２１５において前述の信用度を獲得するための演算を用いることができる。

【０１１４】

ステップ２０５～２０９は、以前のバージョンの扱いを決定するステップである。新しいバージョンのグループ鍵を追加するときには、以前のバージョンのグループ錠を適切に扱う必要がある。これは新しいバージョンのグループ鍵に含まれているＦの値により判断する。Ｆの値にかかわらず、以前のバージョンは古いため、新たに暗号化したり、署名したりすることは行ってはならない。そのため、公開錠リストや、秘密錠リストは、最新のものと、それ以外に分けておくべきである。本実施例においては、その分類は省略し、利用する際に最新という指定をするにとどめている。Ｆの値に応じた対応は次の通りである。

【０１１５】

ａ）Ｆ＝「必要」の場合には、古いバージョンのグループ錠は残される。

ｂ）Ｆ＝「不要」の場合には、古いバージョンのグループ錠は削除される。

ｃ）Ｆ＝「抹消」の場合には、自身が新しいバージョンの秘密鍵を獲得できれば、残される。そうでなければ削除される。

【０１１６】

ステップ２１０～２１３は、公開錠リストへの追加を行い、追加される錠の秘密鍵の利用可能性を判断し、利用可能な場合には、秘密錠リストへの追加も併せて行うことを示すステップである。

【０１１７】

［秘密錠の利用可能性判断］

図１０に秘密鍵の利用可能性を判断するフローを示す。これは指定された任意のグループ錠の中に暗号化されて含まれている秘密鍵を、自身の個人秘密鍵を直接もしくは間接に適用することにより獲得することができるかどうかの判断を行

う処理である。

【０１１８】

この処理は、あるグループ錠を、秘密錠リストに含めて良いか否かの判断（図９のステップ２１２およびステップ２１３）に用いる。他にも、復号の際にグループ鍵を利用可能か否かを判断するためなどにおいて、この処理と同じ判断が必要である。しかし、秘密錠リストに含まれているグループ錠が、その時点において知っている限りにおいて、自身が秘密鍵を獲得できる全てのグループ錠であることを利用して、秘密錠リストに含まれているか否かという簡便な処理で済むことが多く、この処理を直接利用しなければならないことは多くない。

【０１１９】

処理の内容は、まず自身の個人秘密鍵を直接用いて与えられたグループ錠の秘密鍵を獲得できるか否かを判断する。それで獲得できない場合には、自身の秘密錠リスト中の各グループ鍵を直接用いて与えられたグループ錠の秘密鍵を獲得できるか否かを判断する。秘密錠リスト中のグループ錠の秘密鍵を利用可能であることが判明しているので、判断するだけであれば、この手順で処理すれば良い。

【０１２０】

図１０のフローを詳細に説明する。ステップ３０１では、判断の対象とするグループ錠を指定し、ステップ３０２で、自身の個人錠が判断対象であるグループ錠のメンバであるかが検討され、メンバであれば利用可能であるとされる。メンバでない場合は、ステップ３０３からステップ３０５において、現在の秘密錠リストの要素Ｇｉについて検討されＧｉが判断対象の鍵のメンバであるかが検討される。ステップ３０３，３０４，３０５は、Ｇｉのｉを順次インクリメントして繰り返し実行することを意味する。この繰り返しステップ中、いずれかのＧｉが判断対象の鍵のメンバである場合には、利用可能と判断される。

【０１２１】

［暗号化］

図１１に情報の暗号化処理フローを示す。ここで入力するべきものは次の３つである。

ａ）平文

ｂ）復号可能者

公開錠リストに含まれる最新のグループ錠もしくは個人の公開鍵を合わせて一つ以上指定する。

ｃ）署名者

自身の個人秘密鍵か、秘密錠リストに含まれる最新のグループ錠を一つだけ指定する。署名しなければ指定する必要はない。

【０１２２】

署名とは、署名対象であるデータをメッセージダイジェストし、その結果である署名ブロックを秘密鍵によって署名することである。秘密鍵による署名とは、秘密鍵による暗号化である。詳細については、データ構造「暗号」と、データ構造「グループ錠」のＳｉｇ（S_U）の項参照。

【０１２３】

図１１のフローについて詳細に説明する。ステップ４０１では、機密を保持する情報Ｄを入力し、ステップ４０２で、復号を可能とする最新のグループおよび個人に対応する公開鍵Ｐｉを、自身の公開錠リストから１つ以上選択する。これは、暗号化されたデータの復号を可能とするメンバを選択するものである。

【０１２４】

ステップ４０３では、共通鍵Ｋを生成し、Ｋを鍵とする共通鍵暗号方式による情報Ｄの暗号化を実行する。これは前述の［暗号］の欄で述べたように、公開鍵暗号は、暗号化処理および復号処理が遅いため、共通鍵暗号で平文を暗号化し、その共通鍵のみを公開鍵暗号により暗号化するハイブリッド方式を採用していることによるものである。なお、この共通鍵Ｋは暗号化を行う毎に生成するものでなくてもよく、必要に応じて生成するものであったり、あるいは予め決められた固定的なものであってもよい。

【０１２５】

ステップ４０４ではＫを各復号可能者の公開鍵Ｐｉで暗号化しＰｉ（Ｋ）を生成し、それぞれに対応するラベルを付与する。ステップ４０５でその生成された暗号に対する署名を行うか判断し、行わない場合は、ステップ４１０で各データのまとめを実行し、暗号化処理を終了する。署名を実行する場合は、ステップ４

０６に進む。

【０１２６】

ステップ４０６～４０９は署名の処理ステップであり、署名を行うデータのメッセージダイジェスト処理（ステップ４０６）を行い、署名用の鍵を秘密錠リストから選択（ステップ４０７）し、選択した秘密鍵による署名を実行（ステップ４０８）し、配列Ｋ（Ｄ）と署名済みメッセージダイジェスト（＝署名ブロック）をまとめる（ステップ４０９）処理である。以上のステップにより暗号化処理が終了する。

【０１２７】

［復号可能性判断］

図１２に任意の暗号を自身が復号可能であるか否かを判断する処理フローを示す。このフローは、例えば、暗号ファイルのリストをしたとき、自身が復号可能なものがどれであるのかを確認したいとき等に使用される。このフローは復号可能性の判断を高速に実行する処理である。具体的には、ラベルが一致しなければ復号できないことを利用し、まずラベルの一致を確認し、ラベルが一致した場合に限り復号を試みる。一般にラベルの選定方法を適切に決めれば、この方法で十分な性能が得られる。もしラベルの選定方法を規定できないならば、「暗号」にラベルだけでなく、暗号化に利用した公開錠を付与することにより、高速化する方法もある。

【０１２８】

処理は、まず自身の個人秘密鍵の適用を試み、復号できなければ自身の秘密錠リスト中の各グループ錠の適用を試みる。ここにおける復号は、「暗号」中のラベルＬｉに対応するＰｉ（Ｋ）のみの復号である。ここでは、平文を得ることは目的ではないので、Ｋ（Ｄ）の復号は行わない。

【０１２９】

図１２の復号可能性判断フローについて詳細に説明する。ステップ５０１で復号可能性を判断する暗号を指定する。ステップ５０２、５０３で暗号中のラベルＬｉと自身の個人錠のラベルとの一致があるかが判断される。一致がある場合は、ステップ５０９へ進み、復号を試みる。ここで復号できない場合、およびステ

ップ５０２、５０３において一致するラベルがなかった場合は、ステップ５０４、５０５において所有する秘密錠ラベルとの一致が判断される。一致するラベルL_{Gi}があったときは、ステップ５１１に進み、ラベルL_{Gi}に対応するＧｉの秘密鍵$S_{G}i$を獲得し、ステップ５１２，５１３で復号を試みる。復号が成功しない場合は、ステップ５０６，５０７に進み、他の所有秘密錠リストのラベルとの一致および個人錠のラベルとの一致について調べることとなる。なお、ステップ５０６はステップ５０４と同一の処理を異なるラベルについて繰り返すことを示し、ステップ５０７はステップ５０２について異なるラベルについて繰り返すことを示している。ステップ５１０あるいは、ステップ５１３において復号できたときは、ステップ５１４で復号できるとの判断がなされる。

【０１３０】

［グループ錠中の秘密鍵の獲得］

図１３に秘密錠リスト中に存在するグループ錠の秘密鍵S_{G}を獲得するフローを示す。グループ錠の秘密鍵は暗号情報の復号や署名の際などに用いる。

【０１３１】

秘密錠リストには、個人の秘密鍵を直接もしくは間接に適用することにより、その秘密鍵を獲得できるグループ錠のみが含まれているので、獲得できることは明らかである。

【０１３２】

処理は、まず自身の個人秘密鍵を直接適用することを試みる。それが失敗した場合には、秘密錠リスト中のグループ錠を適用することを試みる。グループ錠の適用の試みにおいては、この処理を再帰的に呼び出す。グループをノードとし、メンバというグループ間の包含関係を有向アークとして形成される有向グラフは、ループを持たない。よって、この処理で秘密鍵を獲得することができる。

【０１３３】

図１３の秘密鍵$S_{G}i$の獲得フローについて詳細に説明する。まずステップ６０１で秘密錠リスト中のグループ錠Ｇｉを指定する。ステップ６０２で自身の個人錠がグループ錠Ｇｉのメンバに含まれるかが検討され、含まれる場合は、ステップ６０７に進み、グループ錠Ｇｉ中にある個人公開鍵で共通鍵C_{G}を暗号化し

たＰ$_{Mi}$（Ｃ$_{G}$）を抽出し、これを個人秘密鍵で復号し、共通鍵Ｃ$_{G}$を獲得する。さらに共通鍵Ｃ$_{G}$でグループ錠中のＣ$_{G}$（Ｓ$_{G}$）を復号してグループ秘密鍵Ｓ$_{G}$を獲得する。

【０１３４】

ステップ６０２において、自身の個人錠がグループ錠Ｇｉのメンバに含まれない場合は、ステップ６０３～６０５において、秘密錠リストのすべての要素Ｇｋに対して、ＧｋがＧｉのメンバであるかが検討される。これは、自身の保有する「秘密錠が利用可能なグループ錠Ｇｋ」各々について、グループ錠Ｇｉのメンバとして含まれているかを検討するステップである。ステップ６０４でグループ錠Ｇｉのメンバであるが検出されたときは、ステップ６０８でＧｋの秘密鍵Ｓ$_{Gk}$を獲得し、ステップ６０９でグループ錠Ｇｉ中にある暗号化したＰ$_{Mj}$（Ｓ$_{G}$）を抽出し、これを秘密鍵Ｓ$_{Gk}$で復号し、グループ秘密鍵Ｓ$_{G}$を獲得する。

【０１３５】

［復号］

図１４に任意の暗号を復号する際のフローを示す。図１４に示すフローは、前述した「復号可能性判断」処理とほぼ等しいフローである。ステップ７０１～７１３は、図１２の復号可能性判断フロー中のステップ５０１～５１３に対応する。ただし、ステップ７１４において、共通鍵暗号の鍵Ｋを用いて、Ｋ（Ｄ）を復号し、平文Ｄを獲得する。暗号文に対して署名がされている場合、必要ならば、平文Ｄを獲得するとともに、署名の確認を行う。

【０１３６】

［署名確認］

図１５に署名確認のフローを示す。署名対象にメッセージダイジェスト処理を施した結果と、署名ブロック（署名処理により付与されたデータ）を署名の際に用いられたとされる秘密鍵に対応する公開鍵で復号した結果と比較する。その２つの結果が等しければ署名が正しくなされ、署名対象が改竄されていないことが確認できる。

【０１３７】

ただし、署名に用いられた秘密鍵に対応する公開鍵を信用していなければなら

ない。自身の公開錠リストに含まれていれば良い。信用していなければ、署名の確認はできない。

【０１３８】

メッセージダイジェストの結果と、復号した結果が等しくないときには、署名対象が改竄されていることが分かる。

【０１３９】

図１５に示す署名確認フローについて説明する。まずステップ８０１で、署名対象をメッセージダイジェストする。メッセージダイジェストとは前述のように、署名の対象範囲を全て暗号化するにはコストがかかるために、対象範囲のデータサイズと独立に、対象範囲の内容に応じて１２８ビット程度の情報を生成する処理である。次にステップ８０２において、署名に使用する秘密鍵に対応する公開鍵の信用について判断する。公開鍵を信用していない場合は、ステップ８０６で署名確認は不可能と判断される。

【０１４０】

ステップ８０２において、公開鍵の信用性が確認されれば、ステップ８０３に進み、署名ブロックを署名の際に用いられたとされる秘密鍵に対応する公開鍵で復号し、ステップ８０４とでメッセージダイジェストとの同一性判断がなされる。これが実際上の署名確認ステップとなる。このステップ８０４において同一性がないと判断されればステップ８０７において署名は正しいものではない。すなわち、署名を行った秘密鍵は正しいものではないと判断される。ステップ８０４においてメッセージダイジェストと復号結果が等しいと判断されれば、ステップ８０５においてその署名は正当に行われたと結論づけられる。

【０１４１】

［グループ錠変更］

図１６にグループ錠の変更フローについて示す。グループ錠の変更には、次の４種類がある。フローチャートにおいて、４本の処理に分岐している部分の左側からの順序で示す。

【０１４２】

Ａ．今から追加

新たにメンバを追加する。追加された新たなメンバは、追加以前に暗号化された暗号を復号することはできない。この場合には、新しい秘密鍵と公開鍵の対を新しいバージョンのグループ錠のS_GとP_Gとする。また、Ｆの値は「必要」となる。よって、新しいバージョンを受け取った個人は、以前のバージョンを削除しない。これは、追加以前に暗号化された暗号を、以前からのメンバが復号するために必要であるためである。

【０１４３】

Ｂ．遡って追加

新たにメンバを追加する。追加された新たなメンバは、追加以前に暗号化された暗号も復号することができる。この場合には、以前のS_GとP_Gをそのまま利用する。そのため、Ｆの値は「不要」となる。よって、新しいバージョンを受け取った個人は、以前のバージョンを削除する。以前に暗号化された暗号を復号する場合にも新しいバージョンを用いれば良い。

【０１４４】

Ｃ．今から削除

既存のメンバを削除する。削除されたメンバは、削除以前に暗号化された暗号を復号することができる。当然、削除以降に暗号化されたものは復号できない。この場合には、新しい秘密鍵と公開鍵の対を新しいバージョンのグループ錠のS_GとP_Gとする。また、Ｆの値は「必要」となる。よって、新しいバージョンを受け取った個人は、以前のバージョンを削除しない。これは、削除以前に暗号化された暗号を、削除されたメンバも含めた以前のメンバが復号するために必要であるためである。

【０１４５】

Ｄ．遡って削除

既存のメンバを削除する。削除されたメンバは、削除以前に暗号化された暗号も復号することができない。この場合には、新しい秘密鍵と公開鍵の対を新しいバージョンのグループ錠のS_GとP_Gとする。また、Ｆの値は「抹消」となる。よって新しいバージョンを受け取った個人は、以前のバージョンを削除しない。これは、削除以前に暗号化された暗号を、削除されたメンバを除いた以前のメンバ

が復号するために必要であるためである。ただし、受け取った個人が新しいバージョンの秘密鍵を獲得できない場合、すなわち削除されたメンバであった場合には、削除する。これは、削除以前に暗号化された暗号も削除されたメンバが復号できないようにするためである。この削除されたメンバが以前のバージョンのグループ錠を削除することは数学的に保証するものではなく、システムとして削除を促進することはできるという性格のものである。

【０１４６】

グループ錠を変更したときには、Ｆの値が意味を持つだけでなく、以前のバージョンの変更用秘密鍵で署名する。これは前述したように、以前のバージョンを信用している場合に、新しいバージョンを自動的に信用できるようにするためである。グループ錠を変更したときには、必要な者に速やかに配布する。

【０１４７】

図１６および図１７に示すグループ錠変更フローについて詳述する。ステップ９０１、９０２において変更するグループ錠を特定し、変更の種類を判別する。ステップ９０２において追加と削除の処理のいずれかを選択することとなるが、メンバの入れ替えのように追加、削除が同時に発生するような場合は、メンバごとに順序を設定して１メンバごとに処理を実行する。

【０１４８】

ステップ９０２において変更がメンバの追加である場合は、ステップ９０３へ進み、公開錠リストから追加するメンバに対応するグループもしくは個人の公開鍵を選択する。次にステップ９０４においてこの追加が現在からの追加でよいか、あるいは過去に遡って追加する必要があるかについて判断される。すなわち、過去の暗号情報の復号を可能とするか否かについてを決定するものである。ステップ９０４の判断が「いいえ」すなわち現時点以降の追加となる場合は、ステップ９０５でグループ公開鍵P_G、グループ秘密鍵S_Gおよび共通鍵C_Gが生成され、ステップ９０６でグループ錠の直前バージョン扱いを示す「Ｆ」を必要と設定する。これは、新たなバージョンのグループ錠と元の旧バージョンのグループ錠が共存することを示している。一方ステップ９０４の判断が「遡って追加」である場合は、ステップ９０７、９０８へ進み、現在変更中のグループ錠のS_G、P_G

、C_Gをそのまま変更されたグループ錠のS_G、P_G、C_Gとして設定し、Ｆを「不要」と設定する。これは、旧バージョンのグループ錠が新バージョンのグループ錠に完全に置き換えられたことを示している。次にステップ９０９で、グループ秘密鍵S_Gを共通鍵C_Uで暗号化しC_G（S_G）を生成し、さらにC_Gを追加メンバを含めたメンバの公開鍵P_{Mi}で暗号化し、P_{Mi}に対応するラベルL_{Mi}をインデックスとするP_{Mi}（C_G）の配列を形成する。

【０１４９】

次にステップ９１０で新しい変更権所有者の設定、ステップ９１１で変更鍵の秘密鍵と公開鍵のペアの生成、ステップ９１２で新たな変更権所有者の公開鍵を用いて変更鍵の秘密鍵を暗号化する。

【０１５０】

さらに、ステップ９１３でバージョン番号Ｖの更新、ステップ９１４で各データの一体化、ステップ９１５で一体化されたデータに対する変更秘密鍵による署名を実行し、署名結果Ｓｉｇ（S_U）とし、ステップ９１６でさらに署名結果を加えたデータの一体化を行う。ステップ９１７で、変更前バージョンの変更用秘密鍵S_U'で署名し、Ｓｉｇ（S_U'）とし、ステップ９１８で変更されたグループ錠を作成者の信用錠リストに追加してグループ錠の変更手続を終了する。

【０１５１】

ステップ９０２において変更がメンバの削除である場合は、ステップ９１９へ進み、削除するメンバを選択する。次にステップ９２０においてこの削除が現在からでよいか、あるいは過去に遡る必要があるかについて判断される。すなわち、過去の暗号情報の復号を可能とするか否かについてを決定するものである。ステップ９２０の判断が「いいえ」すなわち現時点以降の削除となる場合は、ステップ９２１でグループ公開鍵P_G、グループ秘密鍵S_G、共通鍵C_Gが生成され、ステップ９２２でグループ錠の直前バージョン扱いを示す「Ｆ」を必要と設定する。これは、新たなバージョンのグループ錠と元の旧バージョンのグループ錠が共存することを示している。一方ステップ９２０の判断が「遡って削除」である場合は、ステップ９２３、９２４へ進み、現在変更中のグループ錠のS_G、P_G、C_Gをそのまま変更されたグループ錠のS_G、P_G、C_Gとして設定し、Ｆを「抹消

」と設定する。次にステップ９２５で、グループ秘密鍵S_Gを共通鍵C_Gで暗号化し、さらに共通鍵C_Gを、削除メンバを削除したたメンバの公開鍵P_{Mi}で暗号化し、P_{Mi}に対応するラベルL_{Mi}をインデックスとするP_{Mi}（C_G）の配列を形成する。以下の手続きであるステップ９１０以降は追加の場合と同様である。

【０１５２】

［実装例］

図１８は、実施例の暗号化方式を実装したシステム例を示している。図１８において、ネットワーク１０には複数のクライアント２０、ファイル・サーバ３０、ディレクトリ・サーバ４０が接続されている。ネットワーク１０はＬＡＮでもよいし、ＷＡＮでもよい。ファイル・サーバ３０は文書等のファイルを保管するものである。ディレクトリ・サーバ４０はグループ錠を保管している。このような構成において、例えばクライアント２０ａがファイル・サーバ３０に文書を保管する場合を考える。クラインんと２０ａは、ディレクトリ・サーバ４０から所望のグループ錠を取出してそこに含まれる公開鍵で文書を暗号化し、暗号化した文書５０ａをファイル・サーバ３０に保管する。この文書をクライアント２０ｂが利用する場合には、クライアント２０ｂはファイル・サーバ３０から文書５０ａを取出すとともにディレクトリ・サーバ４０から所望のグループ錠を取出して秘密鍵を取得し、この秘密鍵で上述の文書を復号する。

【０１５３】

この構成においてクライアント２０ａが文書に署名を付し、署名付き文書５０ｂをファイル・サーバ３０に保管する場合には、クライアント２０ａは所望のグループ錠をディレクトリ・サーバ４０から取出し、グループ錠の秘密鍵を取得し、この秘密鍵で署名を行なう。クライアント２０ｂは、グループ錠の公開鍵を用いて文書の署名を検証できる。

【０１５４】

なお、図１８においては、ファイル・サーバ３０の文書がグループ錠による処理の対象であったが、ファイル・サーバ３０に代えてメール・サーバを用いる場合にも同様な暗号化・復号処理および署名・検証処理が行われる。

【０１５５】

以上、本発明の実施例を説明したが、例えば複号錠の生成、あるいは変更は、暗号化装置、復号装置、あるいはその他の第３局における装置等いずれにおいて実行されてもよく、他のこの公開鍵暗号方式において用いられる他の構成要素、例えば各種の錠リスト等についても同様である。

【０１５６】

また、この実施例では、グループ・メンバの秘密鍵で暗号化するものは、ビット数が小さい（例えば４８～１２０ビット）共通鍵であるので、暗号化の処理量が少なく、メンバの数が多い場合でも迅速にかつ少ないコストでグループ錠を生成できる。また、グループ錠の秘密鍵はグループ錠中、共通鍵で暗号化された暗号文として１度しか現れないので、機密性を保持する上でも好ましい。

【０１５７】

なお、この実施例のグループ錠では、共通鍵でグループ錠の秘密鍵を暗号化しているので、公開鍵で暗号化する場合に比べて低コストで暗号文の解読が可能である。そこで、秘密鍵S_G、S_Uを直接に共通鍵C_G、C_Uで暗号化するのではなく、変形した秘密鍵（S_G'、S_U'）をC_G、C_Uで暗号化するようにしてもよい。

変形した秘密鍵と元の秘密鍵との関係は次のように規定できる。

【数４】

$$S_G' = f_G(S_G)$$
$$S_U' = f_U(S_U)$$

ここで関数f_G、f_Uは一方向でない関数とする。したがって、関数f_G、f_Uには次式のような逆関数f_G^{-1}、f_U^{-1}が存在する。

【数５】

$$S_G = f_G^{-1}(S_G')$$
$$S_U = f_U^{-1}(S_U')$$

変形関数f_G、f_Uは、逆関数が存在すればどのようなものでもよい。機密性の程度に応じて選択することができる。

【０１５８】

このようにすると、攻撃者は、暗号文$C_G(S_G')$、$C_U(S_U')$を解読してS_G'、S_U'を取得しても、逆関数f_G^{-1}、f_U^{-1}を知らないので、秘密鍵S

$_G$、S_Uを取得するのが困難である。

【０１５９】

また、グループ・メンバの公開鍵で共通鍵C_G、C_Uを暗号化して暗号文P_{Mi}（C_G）、P_{Mi}（C_U）を作る代わりに、平文にいわゆるシードをつけて暗号化したものを用いてもよい。これは以下の様なものである。

【数６】

$$P_{Mi}(C_G + f_P(P_{Mi}))$$

$$P_{Mi}(C_U + f_P(P_{Mi}))$$

なお、f_Pは暗号化する公開鍵を入力し何らかのものを出力する関数であり、例えばＭＤ５、ＳＨＡ１（商品名）のようなハッシュ関数を用いることができる。公開鍵はメンバごとに異なるので暗号化対象がメンバ毎に異なり、この結果、安全度を向上させることができる。

【０１６０】

上述の実施例では、グループ・メンバのそれぞれの公開鍵により共通鍵を暗号化しているので、グループ錠中に複数のC_Gの暗号文が現れる。このような場合でも、シードにより、攻撃者にヒントを与えずに済む。

【０１６１】

なお、上述実施例では、秘密鍵を共通鍵で暗号化し、共通鍵をメンバの公開鍵で暗号化したが、秘密鍵をメンバの公開鍵で直截に暗号化するような暗号化スキームも考えられる。このようなスキームでも、上述のようなシードを用いることが可能である。すなわち、秘密鍵S_G、S_Uをメンバの公開鍵P_{Mi}で暗号化したP_{Mi}（S_G）、P_{Mi}（S_U）を含むようにグループ錠を構成する（共通鍵C_G、C_Uは用いない）。そして、この場合にも、P_{Mi}（S_G）、P_{Mi}（S_U）に代えて、シードを入れたP_{Mi}（$S_G + f_P(P_{Mi})$）、P_{Mi}（$S_U + f_P(P_{Mi})$）をグループ錠に含ませるようにすることができる。

【０１６２】

【発明の効果】

以上説明したように、本発明のグループ型公開鍵暗号方式においては、従来の個人を単位とする公開鍵暗号方式にグループの概念を導入し、グループに属する

任意のメンバによる平文の暗号化処理、および暗号情報の復号処理をグループを単位として生成されたグループ公開鍵、グループ秘密鍵、および個人の公開鍵および秘密鍵とを組み合わせて用いることによって実行可能とした。この構成により、グループ内と外との間では高度な機密性を保ちながら、グループ内のメンバ間ではメンバであることの確認の基に暗号情報を共有することを可能とした。また、グループに属するメンバによる電子署名により、グループ内のメンバによる正当な暗号化処理およびその確認を可能とした。

【０１６３】

さらに、本発明のグループ型公開鍵暗号方式では、グループを構成するメンバの変更に対するグループ錠の変更に際し、グループ公開鍵およびグループ秘密鍵の新たなペアの生成および登録を、メンバの変更時点に応じて実行する構成とし、メンバ変更に対してグループ錠を柔軟に変更できる構成とした。また、グループ錠変更に際しての署名をグループ錠を構成する要素の配列全体に対して行うように設定し、変更の保証を確実なものにした。

【０１６４】

また、比較的データ量が小さい共通鍵をメンバの暗号鍵で暗号化してグループ錠を生成するようにしているので、グループ錠の生成負荷が少なくて済む。また、グループ錠の秘密鍵自体は共通鍵で暗号化された態様で１度しかグループ錠に現れないので、攻撃者に対して解読のヒントを与えない。

【図面の簡単な説明】

【図１】　複合錠の信用レベルを決定する演算規則を示した図である。

【図２】　信用体に対する信用レベルとその信用体が有する他のものへの信用レベルから、該他のものの信用レベルを決定するの演算規則を示す図である。

【図３】　本発明の暗号方式全体の概要を示す構成図である。

【図４】　本発明のグループ錠の構成を示す図である。

【図５】　本発明の公開錠リストの構成を示す図である。

【図６】　本発明の秘密錠リストの構成を示す図である。

【図７】　本発明の暗号の構成を示す図である。

【図８】　本発明のグループ錠生成フローを示す図である。

【図９】　本発明の錠リストへの追加フローを示す図である。

【図１０】　本発明の秘密錠の利用可能性判断フローを示す図である。

【図１１】　本発明の暗号化フローを示す図である。

【図１２】　本発明の復号可能性判断フローを示す図である。

【図１３】　本発明の秘密錠リスト中の秘密鍵の獲得フローを示す図である。

【図１４】　本発明の復号フローを示す図である。

【図１５】　本発明の署名確認フローを示す図である。

【図１６】　本発明のグループ錠変更フローを示す図（その１）である。

【図１７】　本発明のグループ錠変更フローを示す図（その２）である。

【図１８】　本発明が適用されるシステムを示す図である。

【符号の説明】

１０１　　個人

１０２　　平文

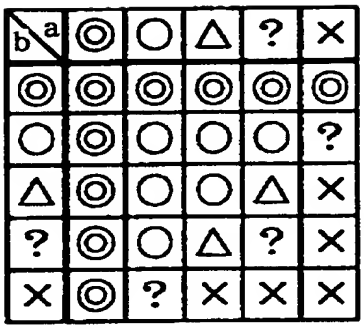
１０３　　暗号

１０４　　錠リスト

１０５　　個人秘密鍵

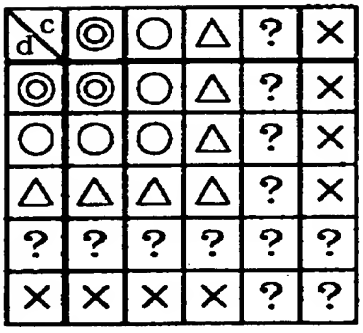
【書類名】　　図面

【図１】



a：個人Ａの信用レベル
b：個人Ｂの信用レベル

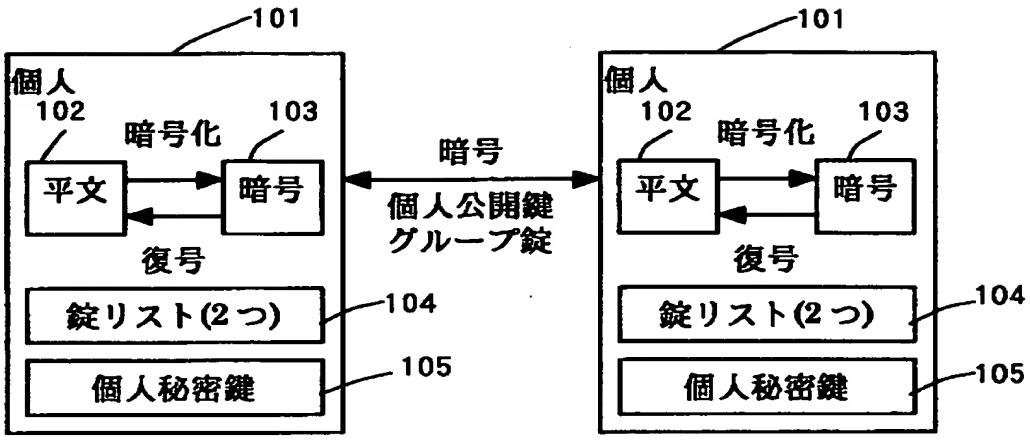
【図２】



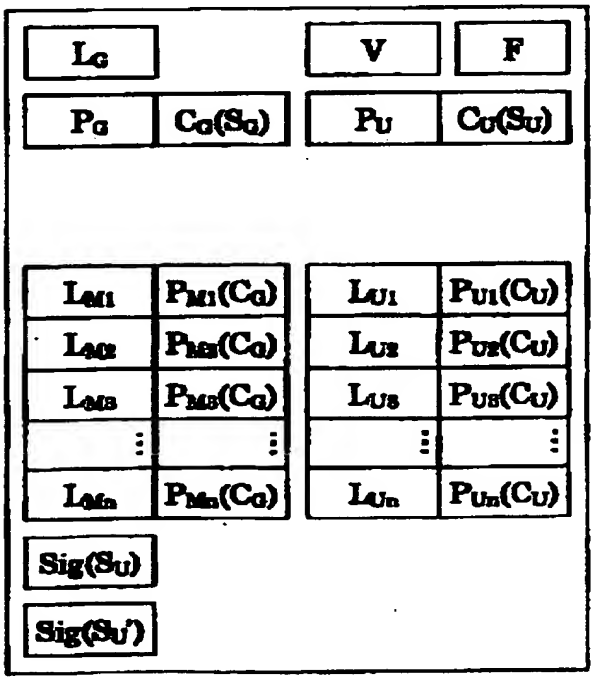
c：信用体に対する信用レベル
d：その信用体の他の信用体に
対する信用レベル

出証特平１１－３０４９０１０

【図３】

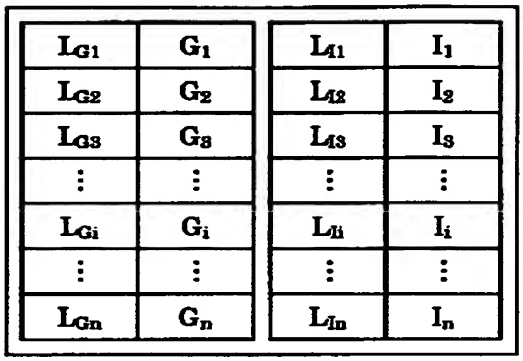


【図４】



出証特平１１－３０４９０１０

【図５】



L_{G1}	G_1	L_{I1}	I_1
L_{G2}	G_2	L_{I2}	I_2
L_{G3}	G_3	L_{I3}	I_3
⋮	⋮	⋮	⋮
L_{Gi}	G_i	L_{Ii}	I_i
⋮	⋮	⋮	⋮
L_{Gn}	G_n	L_{In}	I_n

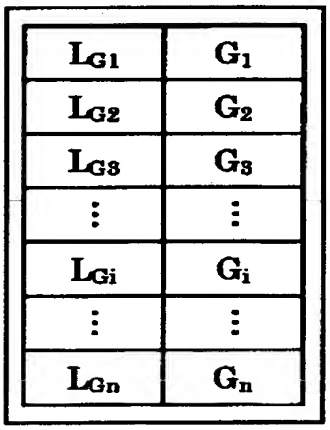
G_i:　　信用しているグループ錠

L_{Gi}:　　グループ錠 G_i のラベル

I_i:　　信用している個人の公開鍵

L_{Ii}:　　個人の公開鍵 I_i に対応するラベル

【図６】

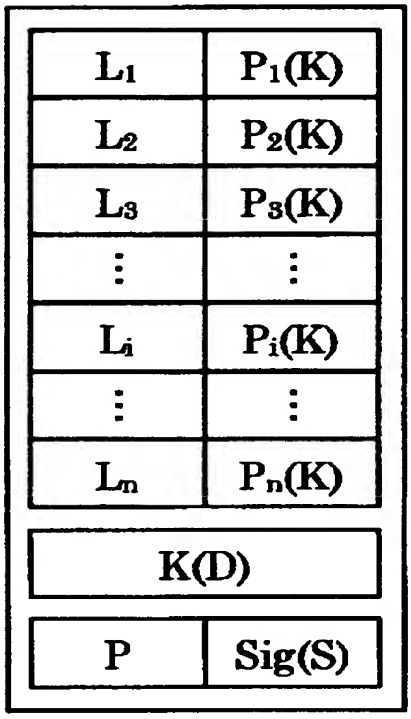


L_{G1}	G_1
L_{G2}	G_2
L_{G3}	G_3
⋮	⋮
L_{Gi}	G_i
⋮	⋮
L_{Gn}	G_n

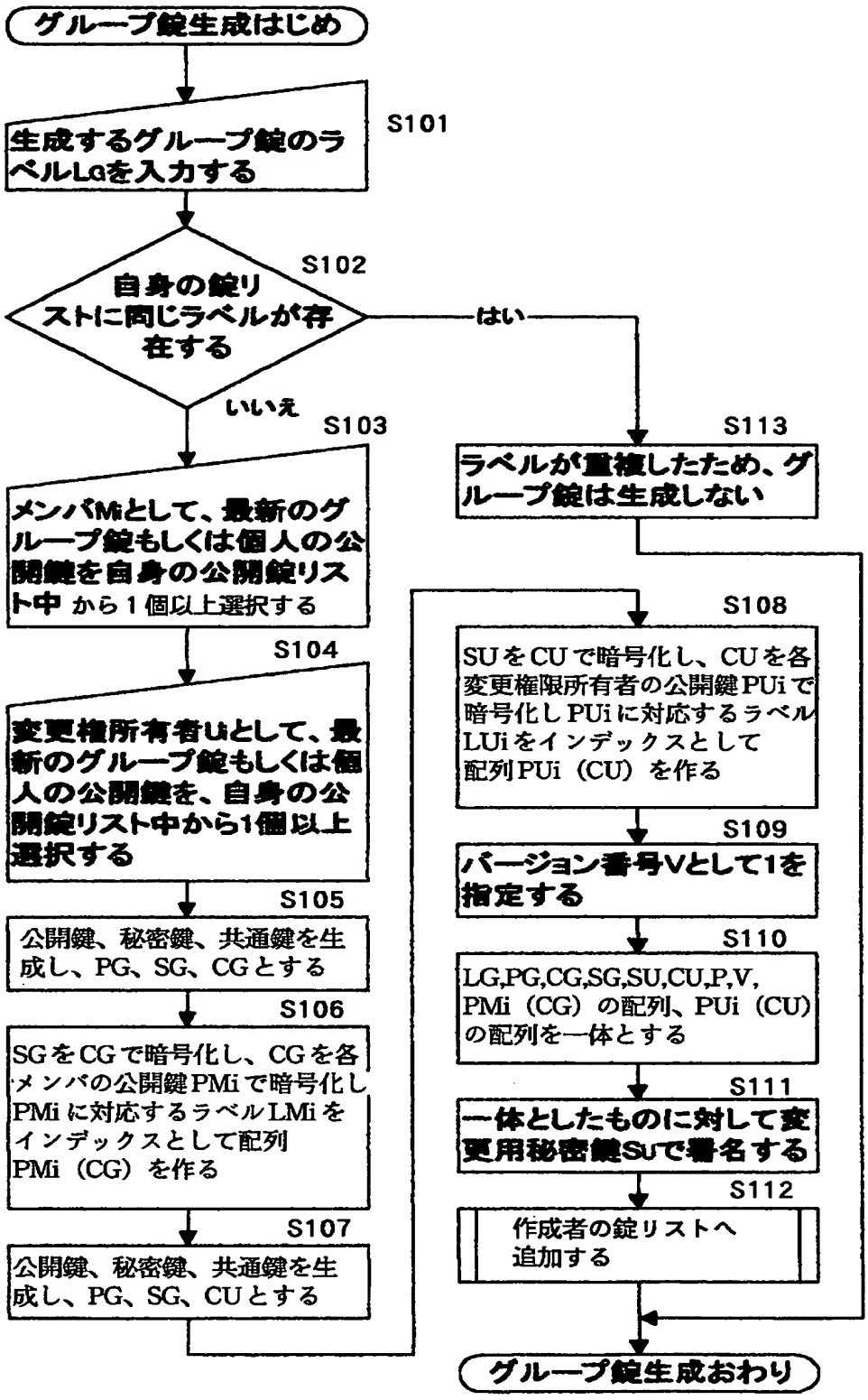
G_i:　　秘密鍵が利用可能なグループ錠

L_{Gi}:　　グループ錠 G_i のラベル

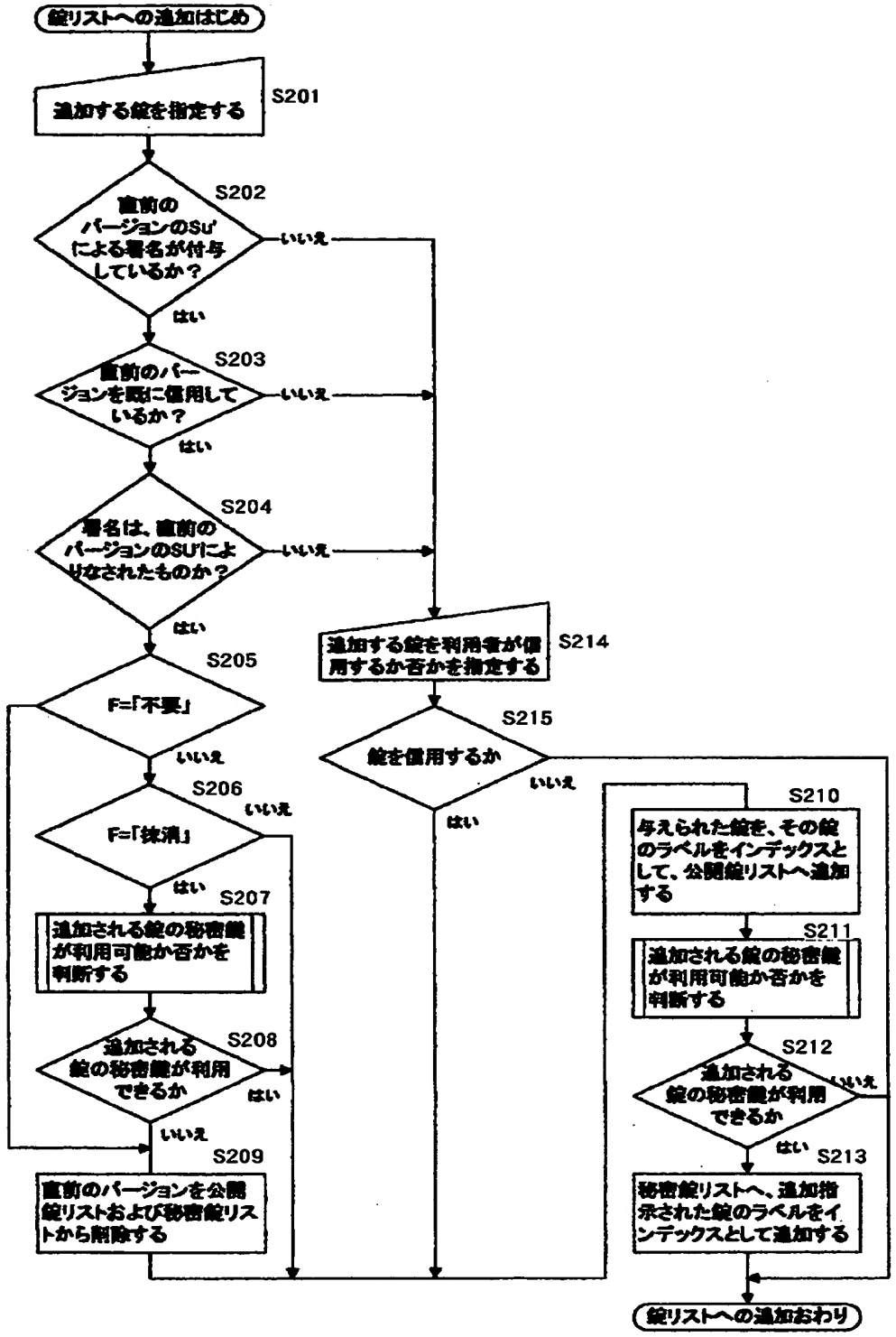
【図７】



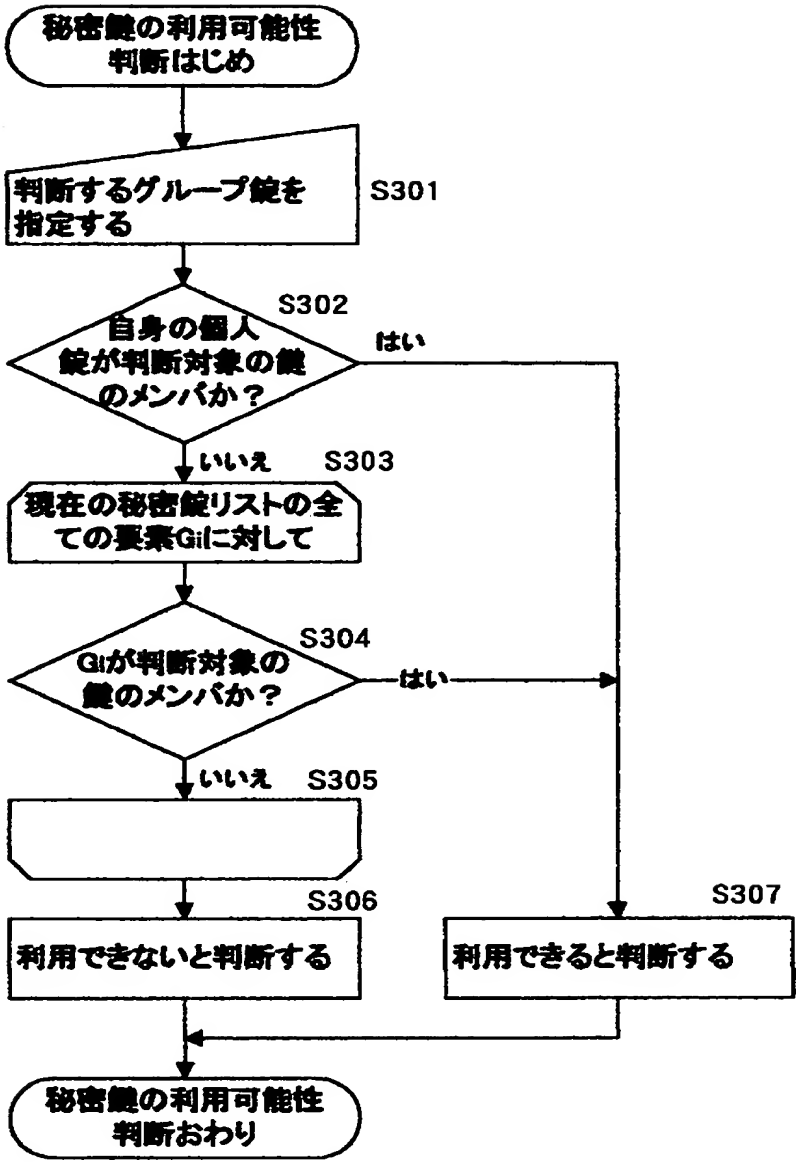
【図８】


グループ錠生成はじめ
生成するグループ錠のラベルLGを入力する
S101
自身の錠リストに同じラベルが存在する
S102
はい
いいえ
S103
メンバMiとして、最新のグループ錠もしくは個人の公開鍵を自身の公開錠リスト中 から１個以上選択する
S104
変更権所有者Uiとして、最新のグループ錠もしくは個人の公開鍵を、自身の公開錠リスト中から1個以上選択する
S105
公開鍵、秘密鍵、共通鍵を生成し、PG、SG、CGとする
S106
SGをCGで暗号化し、CGを各メンバの公開鍵PMiで暗号化しPMiに対応するラベルLMiをインデックスとして配列PMi（CG）を作る
S107
公開鍵、秘密鍵、共通鍵を生成し、PG、SG、CUとする
S113
ラベルが重複したため、グループ錠は生成しない
S108
SUをCUで暗号化し、CUを各変更権限所有者の公開鍵PUiで暗号化しPUiに対応するラベルLUiをインデックスとして配列PUi（CU）を作る
S109
バージョン番号Vとして1を指定する
S110
LG,PG,CG,SG,SU,CU,P,V,PMi（CG）の配列、PUi（CU）の配列を一体とする
S111
一体としたものに対して変更用秘密鍵SUで署名する
S112
作成者の錠リストへ追加する
グループ錠生成おわり

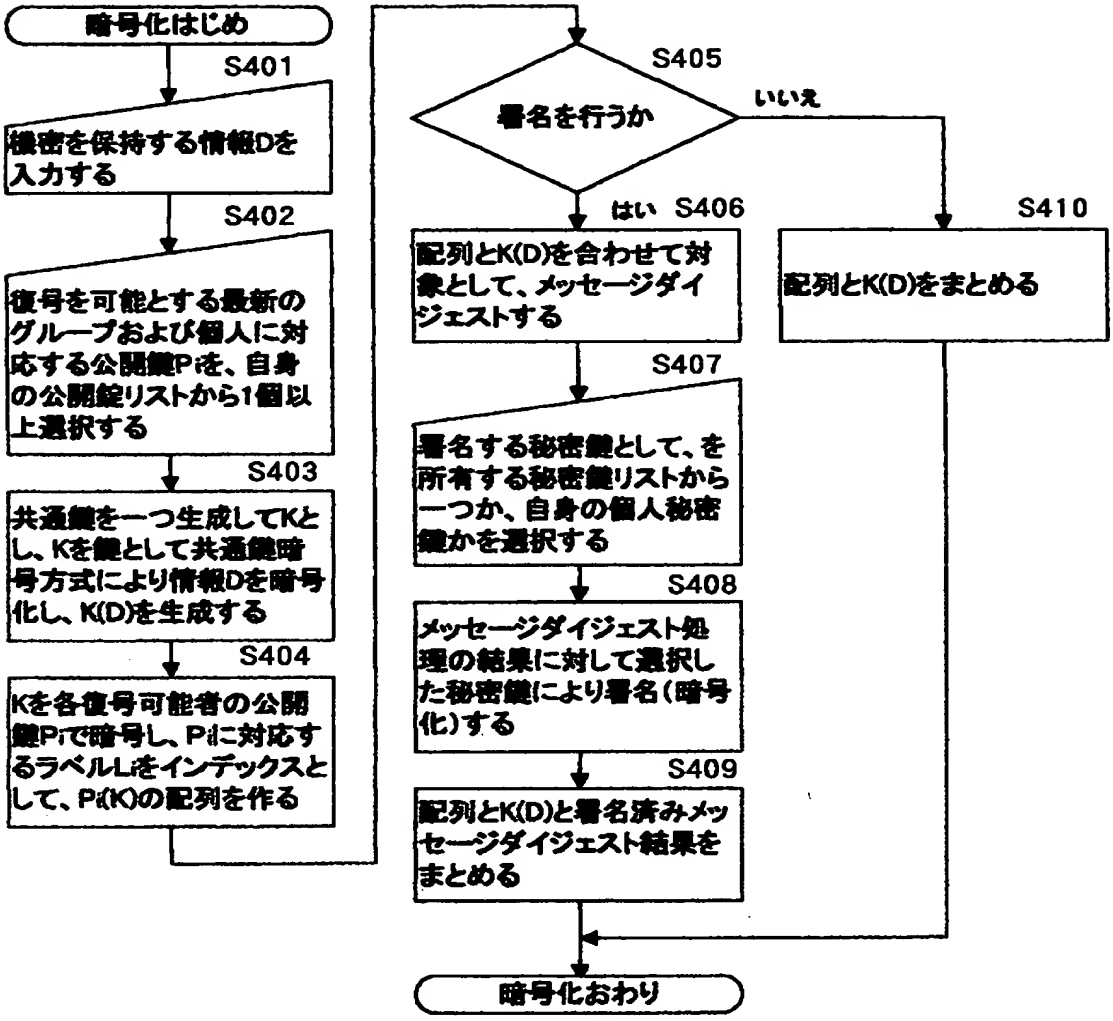
【図９】


錠リストへの追加はじめ
追加する錠を指定する
S201
直前のバージョンのSu'による署名が付与しているか？
S202
いいえ
はい
直前のバージョンを既に僧用しているか？
S203
いいえ
はい
署名は、直前のバージョンのSUによりなされたものか？
S204
いいえ
はい
F=「不要」
S205
いいえ
F=「抹消」
S206
いいえ
はい
追加される錠の秘密鍵が利用可能か否かを判断する
S207
追加される錠の秘密鍵が利用できるか
S208
はい
いいえ
直前のバージョンを公開錠リストおよび秘密錠リストから削除する
S209
追加する錠を利用者が僧用するか否かを指定する
S214
錠を僧用するか
S215
いいえ
はい
与えられた錠を、その錠のラベルをインデックスとして、公開錠リストへ追加する
S210
追加される錠の秘密鍵が利用可能か否かを判断する
S211
追加される錠の秘密鍵が利用できるか
S212
いいえ
はい
秘密錠リストへ、追加指示された錠のラベルをインデックスとして追加する
S213
錠リストへの追加おわり

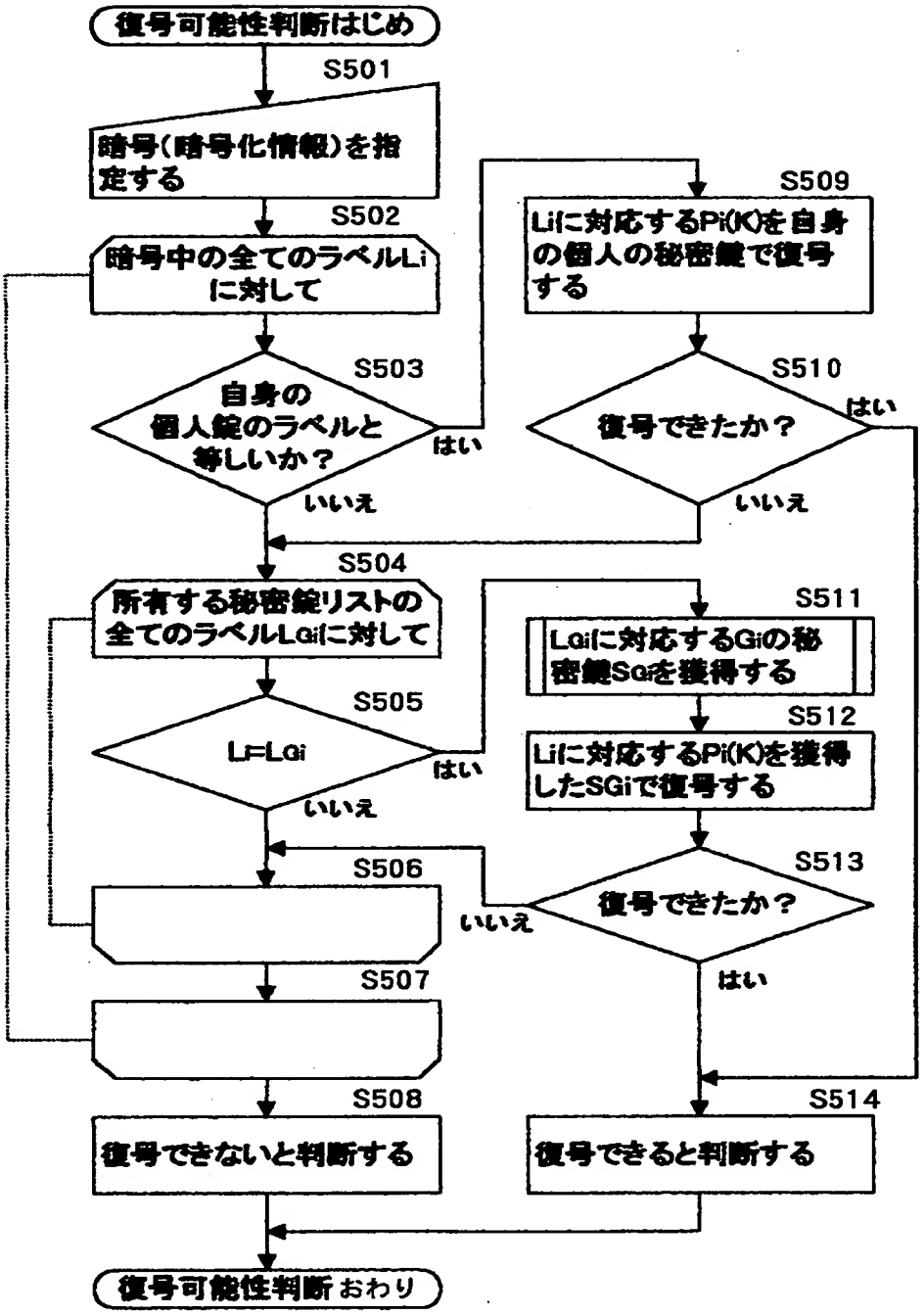
【図１０】


秘密鍵の利用可能性判断はじめ
判断するグループ鍵を指定する
S301
S302
自身の個人鍵が判断対象の鍵のメンバか？
はい
いいえ
S303
現在の秘密鍵リストの全ての要素Giに対して
S304
Giが判断対象の鍵のメンバか？
はい
いいえ
S305
S306
利用できないと判断する
S307
利用できると判断する
秘密鍵の利用可能性判断おわり

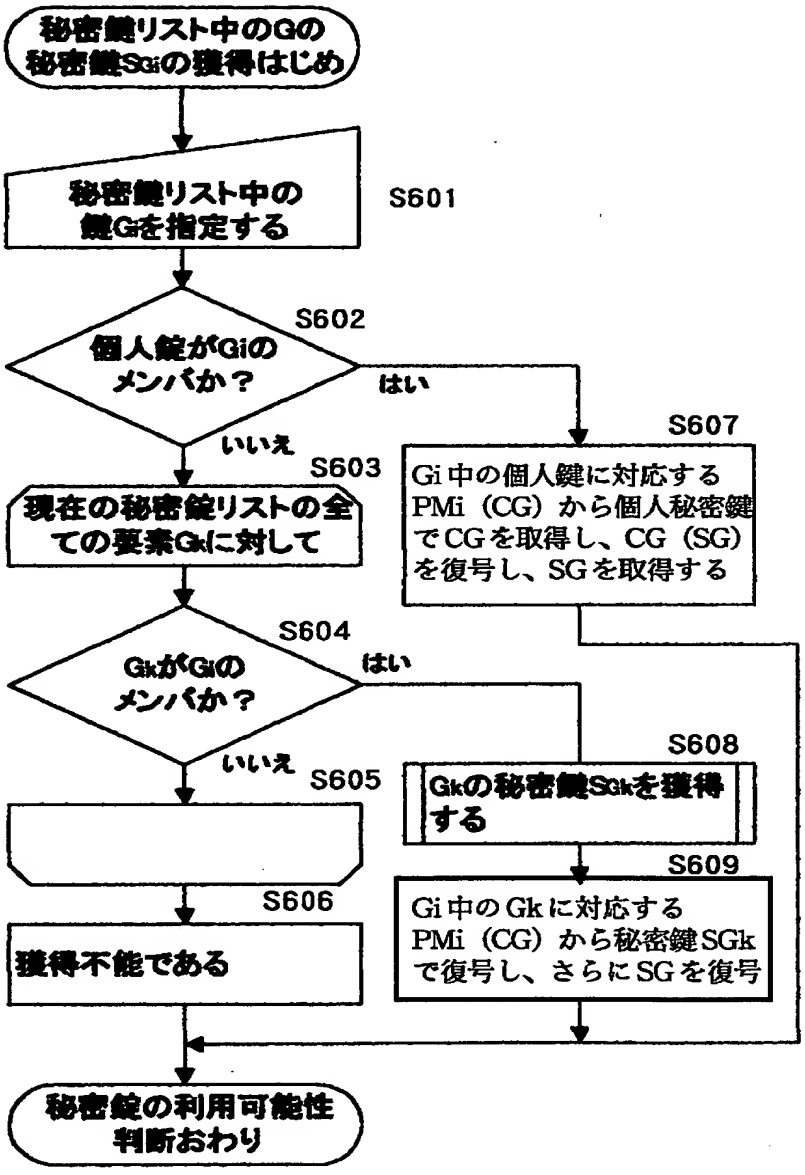
【図１１】


暗号化はじめ
S401
機密を保持する情報Dを入力する
S402
復号を可能とする最新のグループおよび個人に対応する公開鍵Piを、自身の公開鍵リストから1個以上選択する
S403
共通鍵を一つ生成してKとし、Kを鍵として共通鍵暗号方式により情報Dを暗号化し、K(D)を生成する
S404
Kを各復号可能者の公開鍵Piで暗号し、Piに対応するラベルLiをインデックスとして、Pi(K)の配列を作る
S405
署名を行うか
いいえ
はい
S406
配列とK(D)を合わせて対象として、メッセージダイジェストする
S407
署名する秘密鍵として、を所有する秘密鍵リストから一つか、自身の個人秘密鍵かを選択する
S408
メッセージダイジェスト処理の結果に対して選択した秘密鍵により署名(暗号化)する
S409
配列とK(D)と署名済みメッセージダイジェスト結果をまとめる
S410
配列とK(D)をまとめる
暗号化おわり

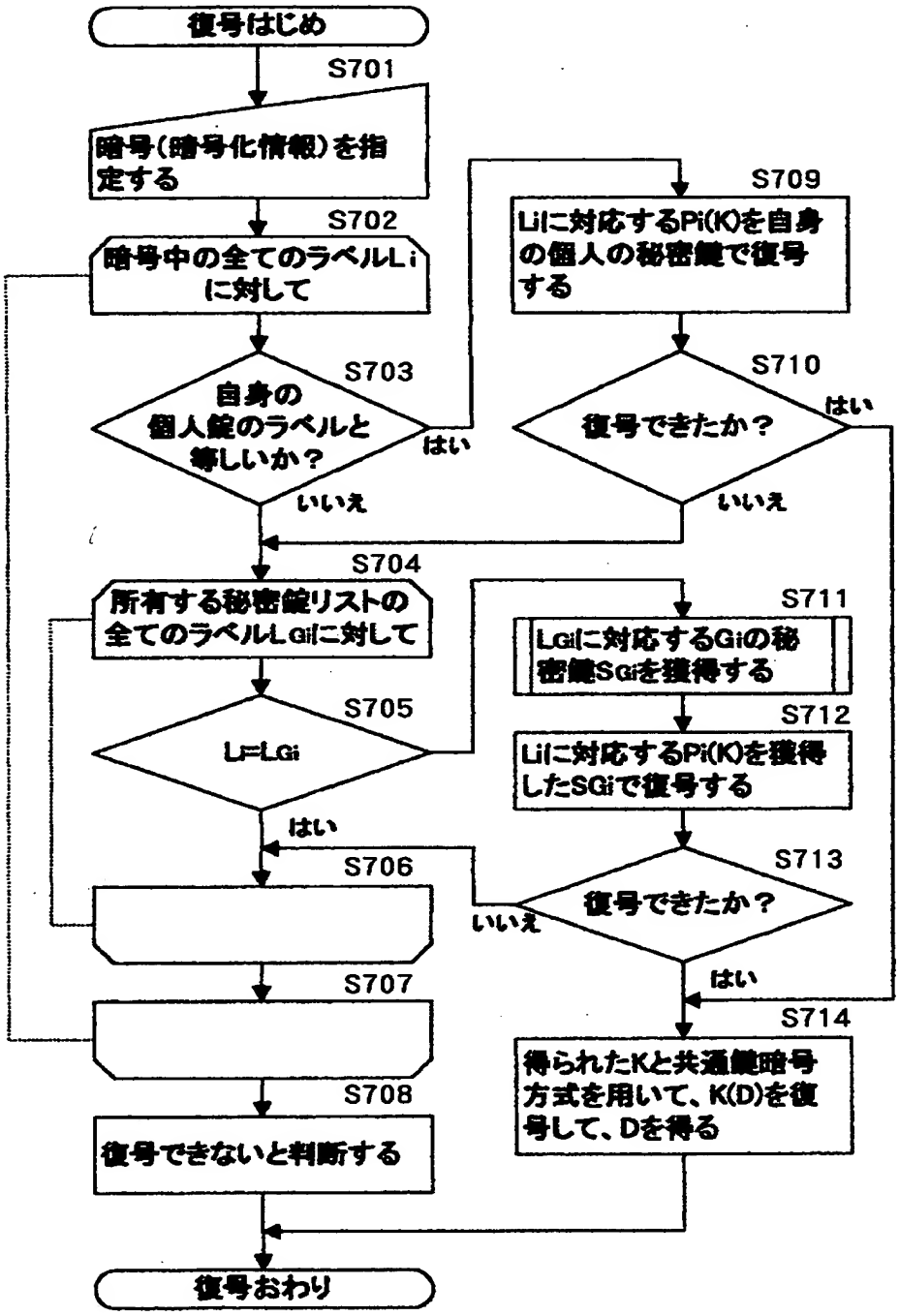
【図１２】


復号可能性判断はじめ
S501
暗号(暗号化情報)を指定する
S502
暗号中の全てのラベルLiに対して
S503
自身の個人鍵のラベルと等しいか？
はい
いいえ
S504
所有する秘密鍵リストの全てのラベルLGiに対して
S505
L=LGi
はい
いいえ
S506
S507
S508
復号できないと判断する
S509
Liに対応するPi(K)を自身の個人の秘密鍵で復号する
S510
復号できたか？
はい
いいえ
S511
LGiに対応するGiの秘密鍵SGiを獲得する
S512
Liに対応するPi(K)を獲得したSGiで復号する
S513
復号できたか？
いいえ
はい
S514
復号できると判断する
復号可能性判断おわり

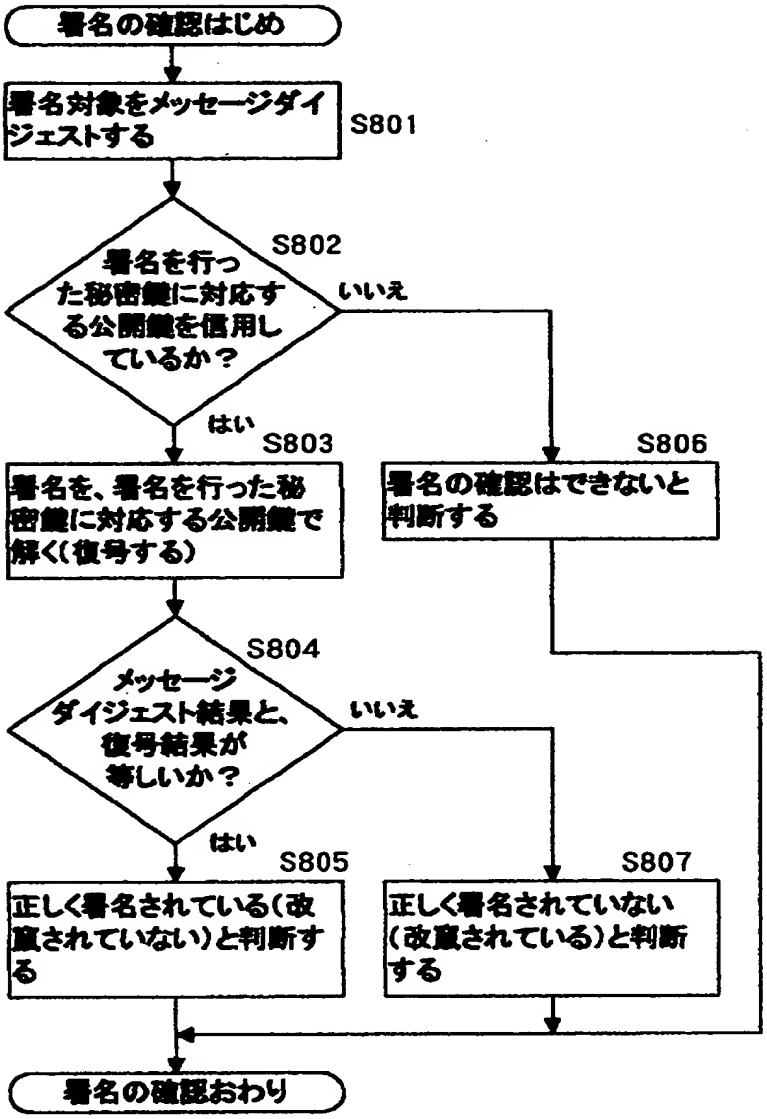
【図１３】


秘密鍵リスト中のGの秘密鍵SGiの獲得はじめ
秘密鍵リスト中の鍵Giを指定する
S601
S602
個人鍵がGiのメンバか？
はい
いいえ
S607
Gi中の個人鍵に対応するPMi（CG）から個人秘密鍵でCGを取得し、CG（SG）を復号し、SGを取得する
S603
現在の秘密鍵リストの全ての要素Gkに対して
S604
GkがGiのメンバか？
はい
いいえ
S608
Gkの秘密鍵SGkを獲得する
S605
S609
Gi中のGkに対応するPMi（CG）から秘密鍵SGkで復号し、さらにSGを復号
S606
獲得不能である
秘密鍵の利用可能性判断おわり

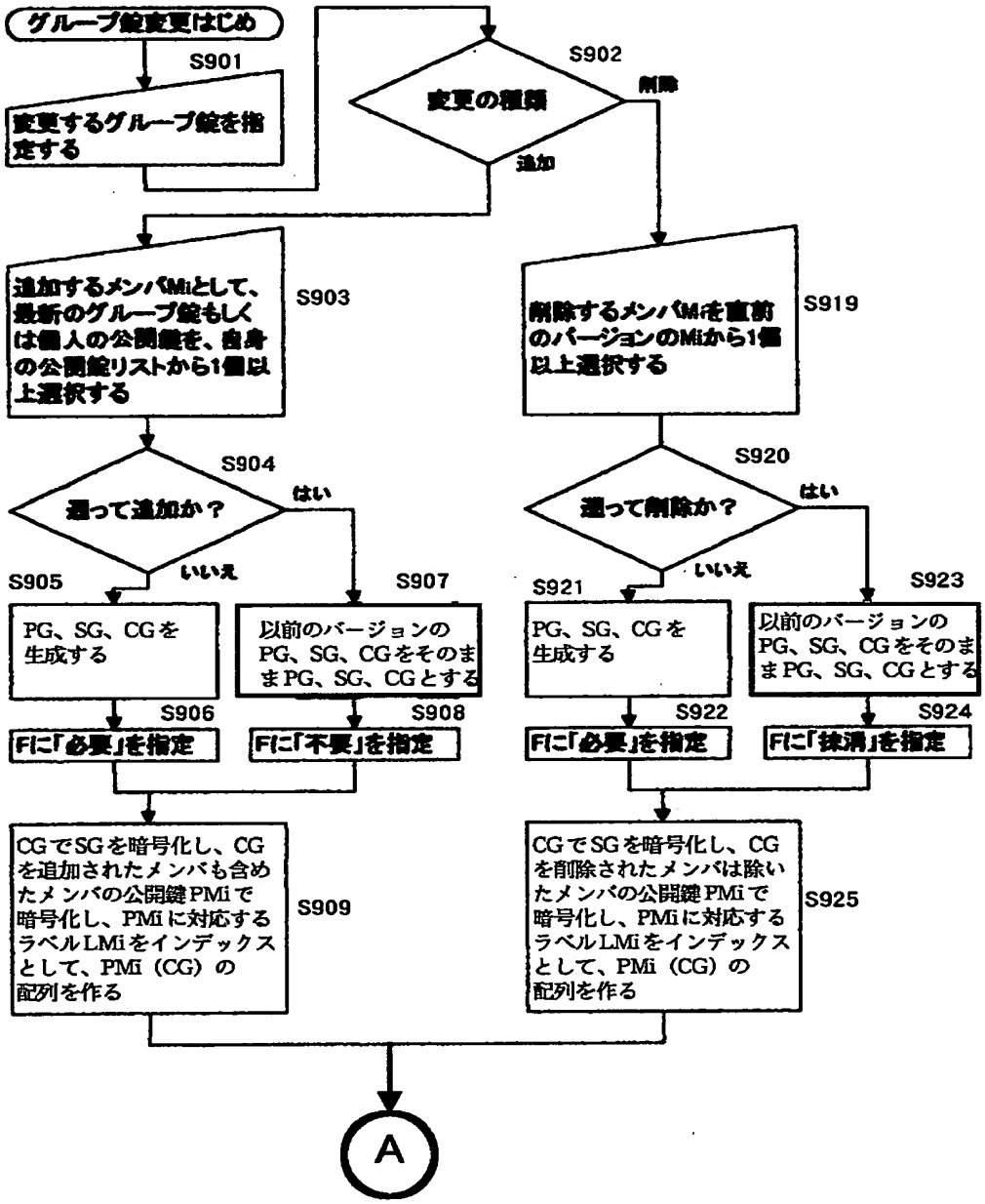
【図１４】


復号はじめ
S701
暗号(暗号化情報)を指定する
S702
暗号中の全てのラベルLiに対して
S703
自身の個人鍵のラベルと等しいか？
はい
いいえ
S704
所有する秘密鍵リストの全てのラベルLGiに対して
S705
L=LGi
はい
S706
S707
S708
復号できないと判断する
S709
Liに対応するPi(K)を自身の個人の秘密鍵で復号する
S710
復号できたか？
はい
いいえ
S711
LGiに対応するGiの秘密鍵SGiを獲得する
S712
Liに対応するPi(K)を獲得したSGiで復号する
S713
復号できたか？
いいえ
はい
S714
得られたKと共通鍵暗号方式を用いて、K(D)を復号して、Dを得る
復号おわり

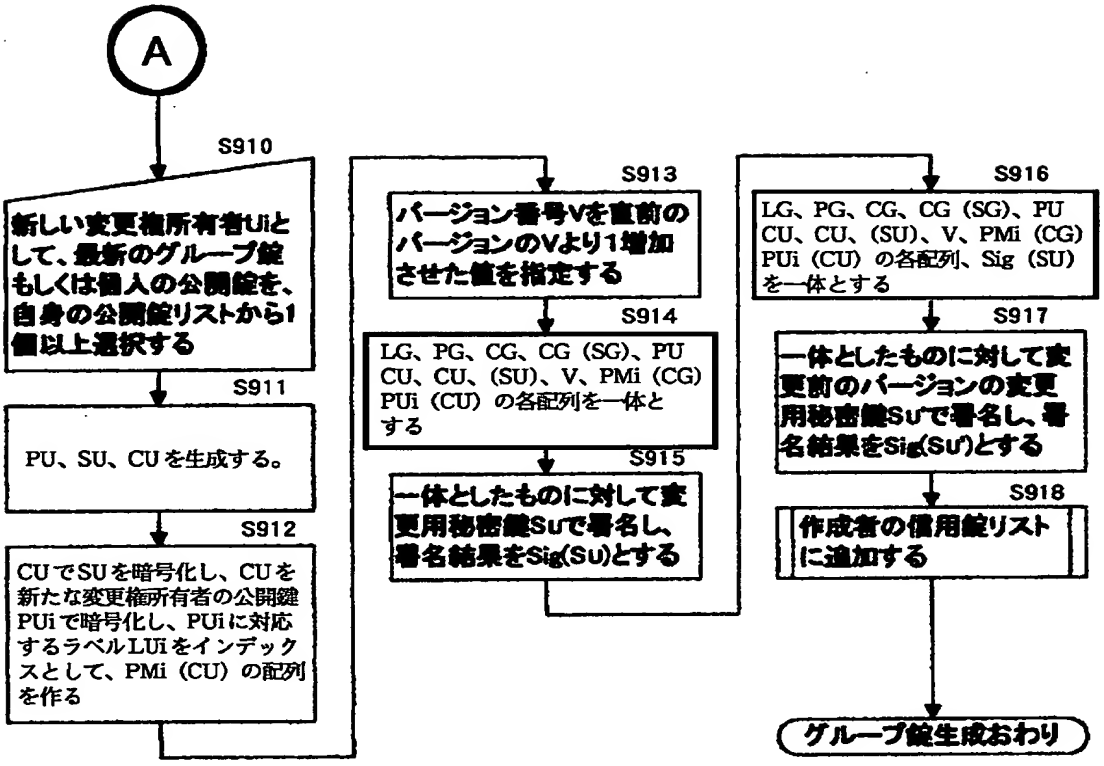
【図１５】


署名の確認はじめ
署名対象をメッセージダイジェストする
S801
署名を行った秘密鍵に対応する公開鍵を信用しているか？
S802
いいえ
はい
S803
署名を、署名を行った秘密鍵に対応する公開鍵で解く(復号する)
S806
署名の確認はできないと判断する
メッセージダイジェスト結果と、復号結果が等しいか？
S804
いいえ
はい
S805
正しく署名されている(改竄されていない)と判断する
S807
正しく署名されていない(改竄されている)と判断する
署名の確認おわり

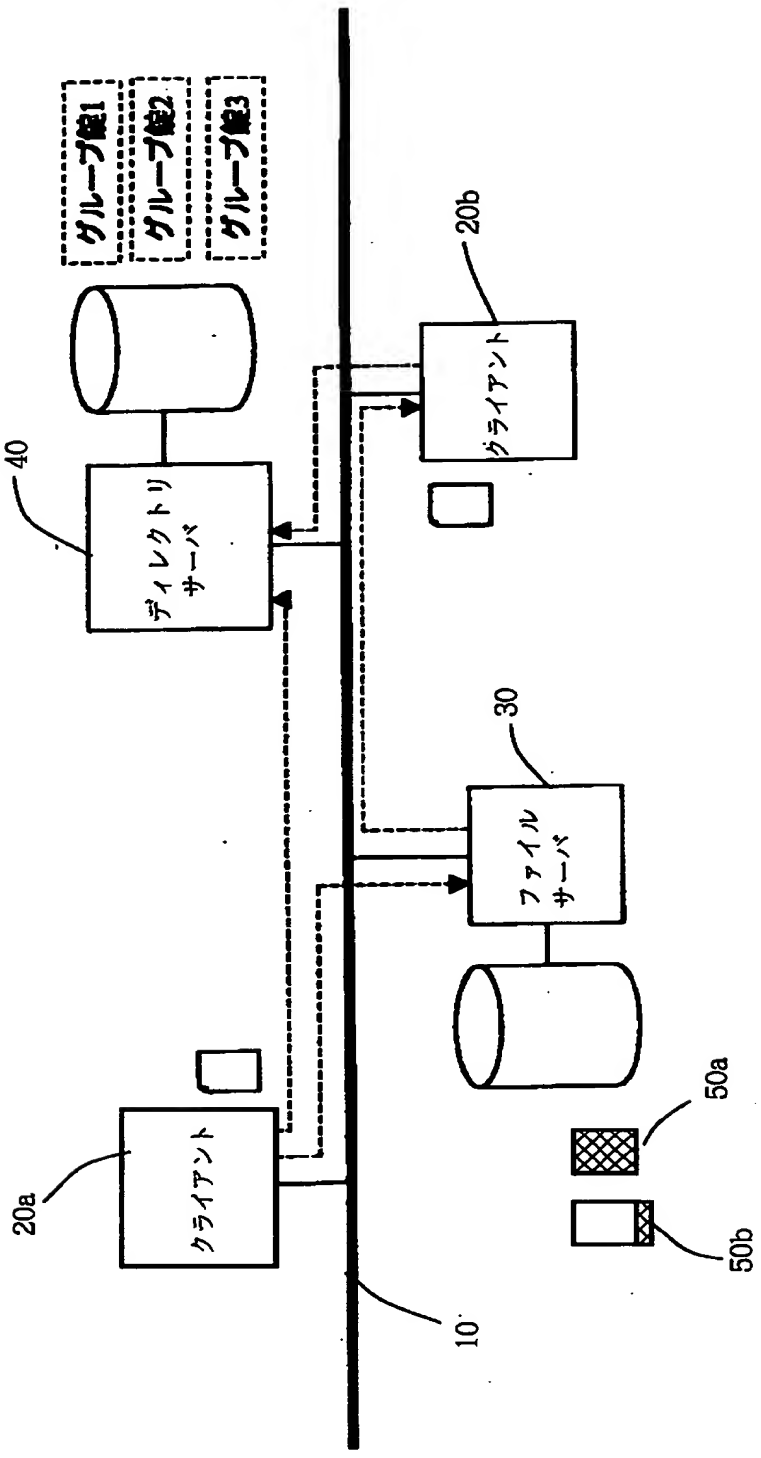
【図１６】


グループ鍵変更はじめ
S901
変更するグループ鍵を指定する
S902
変更の種類
削除
追加
追加するメンバMiとして、最新のグループ鍵もしくは個人の公開鍵を、自身の公開鍵リストから1個以上選択する
S903
S919
削除するメンバMiを直前のバージョンのMiから1個以上選択する
S904
選って追加か？
はい
いいえ
S920
選って削除か？
はい
いいえ
S905
PG、SG、CGを生成する
S907
以前のバージョンのPG、SG、CGをそのままPG、SG、CGとする
S921
PG、SG、CGを生成する
S923
以前のバージョンのPG、SG、CGをそのままPG、SG、CGとする
S906
Fに「必要」を指定
S908
Fに「不要」を指定
S922
Fに「必要」を指定
S924
Fに「抹消」を指定
CGでSGを暗号化し、CGを追加されたメンバも含めたメンバの公開鍵PMiで暗号化し、PMiに対応するラベルLMiをインデックスとして、PMi（CG）の配列を作る
S909
CGでSGを暗号化し、CGを削除されたメンバは除いたメンバの公開鍵PMiで暗号化し、PMiに対応するラベルLMiをインデックスとして、PMi（CG）の配列を作る
S925
A

【図１７】


A
S910
新しい変更権所有者Uiとして、最新のグループ鍵もしくは個人の公開鍵を、自身の公開鍵リストから1個以上選択する
S911
PU、SU、CUを生成する。
S912
CUでSUを暗号化し、CUを新たな変更権所有者の公開鍵PUiで暗号化し、PUiに対応するラベルLUiをインデックスとして、PMi（CU）の配列を作る
S913
バージョン番号Vを直前のバージョンのVより1増加させた値を指定する
S914
LG、PG、CG、CG（SG）、PU CU、CU、（SU）、V、PMi（CG）PUi（CU）の各配列を一体とする
S915
一体としたものに対して変更用秘密鍵Suで署名し、署名結果をSig(Su)とする
S916
LG、PG、CG、CG（SG）、PU CU、CU、（SU）、V、PMi（CG）PUi（CU）の各配列、Sig（SU）を一体とする
S917
一体としたものに対して変更前のバージョンの変更用秘密鍵Su'で署名し、署名結果をSig(Su')とする
S918
作成者の信用鍵リストに追加する
グループ鍵生成おわり

【図１８】


グループ鍵1
グループ鍵2
グループ鍵3
40
ディレクトリサーバ
20b
クライアント
30
ファイルサーバ
50a
50b
20a
クライアント
10

【書類名】　要約書

【要約】

【課題】　暗号化・復号や署名を行なうためにグループ単位で利用できるグループ錠を提供する。

【解決手段】　公開鍵、秘密鍵および共通鍵を用意し、秘密鍵を共通鍵で暗号化する。また、共通鍵をグループ・メンバの各公開鍵で暗号化する。公開鍵、秘密鍵の暗号文、共通鍵の複数の暗号文を含ませてグループ錠を形成する。グループ・メンバはグループ錠を取得して、自分の秘密鍵で共通鍵の暗号文を復号し共通鍵を取得し、これでグループ錠の秘密鍵の暗号文を復号して秘密鍵を取得する。グループ・メンバは、グループ錠の公開鍵で暗号化されてグループ宛てに送付されてきた暗号文を取得し、この暗号文を、復号した秘密鍵で復号する。

【選択図】　図４

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005496
【住所又は居所】　東京都港区赤坂二丁目１７番２２号
【氏名又は名称】　富士ゼロックス株式会社
【代理人】　申請人
【識別番号】　100086531
【住所又は居所】　東京都中央区新富１－１－７　銀座ティーケイビル７階　澤田・宮田・山田特許事務所
【氏名又は名称】　澤田　俊夫

出　願　人　履　歴　情　報

識別番号　　〔０００００５４９６〕

１．変更年月日　　１９９６年　５月２９日
［変更理由］　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社